Motorola Solutions WiNG 5

CLI REFERENCE GUIDE

MOTOROLA SOLUTIONS WING 5
CLI REFERENCE GUIDE

72E-152229-01

Revision B

May 2011

No part of this publication may be reproduced or used in any form, or by any electrical or mechanical means, without permission in writing from Motorola. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice.

The software is provided strictly on an “as is” basis. All software, including firmware, furnished to the user is on a licensed basis. Motorola grants to the user a non-transferable and non-exclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Motorola. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Motorola. The user agrees to maintain Motorola’s copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof.

Motorola reserves the right to make changes to any software or product to improve reliability, function, or design.

Motorola does not assume any product liability arising out of, or in connection with, the application or use of any product, circuit, or application described herein.

No license is granted, either expressly or by implication, estoppel, or otherwise under any Motorola, Inc., intellectual property rights. An implied license only exists for equipment, circuits, and subsystems contained in Motorola products.

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev A	May 2011	Original WING 5.1 release.
-01 Rev B	May 2011	Corrected issue with Front Page. Changed revision to B

TABLE OF CONTENTS

About This Guide 13

Chapter 1, INTRODUCTION ---------- 1-1
1.1 CLI Overview 1-3
1.2 Getting Context Sensitive Help 1-7
1.3 Using the No Command 1-9
1.3.1 Basic Conventions 1-9
1.4 Using CLI Editing Features and Shortcuts 1-10
1.4.1 Moving the Cursor on the Command Line 1-11
1.4.2 Completing a Partial Command Name 1-12
1.4.3 Command Output pagination 1-12
1.4.4 Creating Profiles 1-12
1.4.5 Change the default profile by creating vlan 150 and mapping to ge3 Physical interface 1-13
1.4.6 Remote Administration 1-13

Chapter 2, USER EXEC MODE COMMANDS ---------- 2-1
2.1 User Exec Commands 2-2
2.1.1 ap-upgrade 2-4
2.1.2 change-passwd 2-7
2.1.3 clear 2-8
2.1.4 clock 2-11
2.1.5 clrscr 2-12
2.1.6 cluster 2-13
2.1.7 commit 2-14
2.1.8 connect 2-15
2.1.9 crypto 2-16
2.1.10 disable 2-25
2.1.11 enable 2-26
2.1.12 exit 2-27
2.1.13 help 2-28
2.1.14 logging 2-32
2.1.15 mint 2-33

2.1.16 no 2-35
2.1.17 page 2-36
2.1.18 ping 2-37
2.1.19 revert 2-38
2.1.20 service 2-39
2.1.21 show 2-40
2.1.22 telnet 2-42
2.1.23 terminal 2-43
2.1.24 time-it 2-44
2.1.25 traceroute 2-45
2.1.26 watch 2-46
2.1.27 write 2-47

Chapter 3, PRIVILEGED EXEC MODE COMMANDS ----------3-1
3.1 Privileged Exec Mode Commands 3-3
3.1.1 ap-upgrade 3-5
3.1.2 archive 3-8
3.1.3 boot 3-9
3.1.4 cd 3-10
3.1.5 change-passwd 3-11
3.1.6 clear 3-12
3.1.7 clock 3-15
3.1.8 clrscr 3-16
3.1.9 cluster 3-17
3.1.10 configure 3-18
3.1.11 commit 3-19
3.1.12 connect 3-20
3.1.13 copy 3-21
3.1.14 crypto 3-22
3.1.15 delete 3-31
3.1.16 disable 3-32
3.1.17 diff 3-33
3.1.18 dir 3-34
3.1.19 edit 3-35
3.1.20 enable 3-36
3.1.21 erase 3-37
3.1.22 exit 3-38
3.1.23 format 3-39
3.1.24 halt 3-40
3.1.25 help 3-41
3.1.26 logging 3-45
3.1.27 mkdir 3-46
3.1.28 mint 3-47
3.1.29 more 3-49
3.1.30 no 3-50
3.1.31 page 3-51
3.1.32 ping 3-52
3.1.33 pwd 3-53
3.1.34 reload 3-54
3.1.35 rename 3-55

3.1.36 revert 3-56
3.1.37 rmdir 3-57
3.1.38 self 3-58
3.1.39 service 3-59
3.1.40 show 3-60
3.1.41 telnet 3-62
3.1.42 terminal 3-63
3.1.43 time-it 3-64
3.1.44 traceroute 3-65
3.1.45 upgrade 3-66
3.1.46 upgrade-abort 3-67
3.1.47 watch 3-68
3.1.48 write 3-69

Chapter 4, GLOBAL CONFIGURATION COMMANDS 4-1
4.1 Global Configuration Commands 4-2
4.1.1 aaa-policy 4-4
4.1.2 advanced-wips-policy 4-5
4.1.3 ap650 4-6
4.1.4 ap6511 4-7
4.1.5 ap6532 4-8
4.1.6 ap71xx 4-9
4.1.7 association-acl-policy 4-10
4.1.8 auto-provisioning-policy 4-11
4.1.9 captive portal 4-12
4.1.10 clear 4-29
4.1.11 critical-resource-policy 4-30
4.1.12 customize 4-35
4.1.13 device 4-40
4.1.14 device-categorization 4-41
4.1.15 dhcp-server-policy 4-46
4.1.16 dns-whitelist 4-47
4.1.17 do 4-52
4.1.18 end 4-54
4.1.19 event-system-policy 4-55
4.1.20 firewall-policy 4-69
4.1.21 help 4-70
4.1.22 host 4-72
4.1.23 igmp-snoop-policy 4-73
4.1.24 ip 4-74
4.1.25 mac 4-75
4.1.26 management-policy 4-76
4.1.27 mint-policy 4-77
4.1.28 nac-list 4-78
4.1.29 no 4-84
4.1.30 password-encryption 4-86
4.1.31 profile 4-87
4.1.32 radio-qos-policy 4-89
4.1.33 radius-group 4-90
4.1.34 radius-server-policy 4-91

4.1.35 radius-user-pool-policy 4-92
4.1.36 rf-domain 4-93
4.1.37 rfs4000 4-99
4.1.38 rfs6000 4-100
4.1.39 rfs7000 4-101
4.1.40 role-policy 4-102
4.1.41 self 4-103
4.1.42 service 4-104
4.1.43 show 4-106
4.1.44 smart-rf-policy 4-108
4.1.45 wips-policy 4-109
4.1.46 wlan 4-110
4.1.47 wlan-qos-policy 4-153
4.1.48 write 4-154

Chapter 5, COMMON COMMANDS ----------5-1
5.1 Common Commands 5-2
5.1.1 clrscr 5-3
5.1.2 commit 5-4
5.1.3 exit 5-5
5.1.4 help 5-6
5.1.5 no 5-10
5.1.6 show 5-12
5.1.7 revert 5-14
5.1.8 service 5-15
5.1.9 write 5-35

Chapter 6, SHOW COMMANDS ----------6-1
6.1 show commands 6-2
6.1.1 show 6-5
6.1.2 adoption 6-8
6.1.3 advanced-wips 6-10
6.1.4 ap-upgrade 6-13
6.1.5 boot 6-14
6.1.6 captive-portal 6-15
6.1.7 cdp 6-17
6.1.8 clock 6-18
6.1.9 cluster 6-19
6.1.10 commands 6-20
6.1.11 context 6-22
6.1.12 critical-resources 6-24
6.1.13 crypto 6-25
6.1.14 debug 6-28
6.1.15 debugging 6-30
6.1.16 device-categorization 6-32
6.1.17 event-history 6-33
6.1.18 event-system-policy 6-34
6.1.19 file 6-35
6.1.20 firewall 6-36

6.1.21 interface 6-40
6.1.22 ip 6-42
6.1.23 ip-access-list-stats 6-47
6.1.24 licenses 6-48
6.1.25 lldp 6-49
6.1.26 logging 6-50
6.1.27 mac-access-list-stats 6-51
6.1.28 mac-address-table 6-52
6.1.29 mint 6-53
6.1.30 noc 6-55
6.1.31 ntp 6-57
6.1.32 password-encryption 6-58
6.1.33 power 6-59
6.1.34 remote-debug 6-60
6.1.35 rf-domain-manager 6-61
6.1.36 role 6-62
6.1.37 running-config 6-63
6.1.38 session-changes 6-65
6.1.39 session-config 6-66
6.1.40 sessions 6-67
6.1.41 smart-rf 6-68
6.1.42 spanning-tree 6-70
6.1.43 startup-config 6-73
6.1.44 terminal 6-74
6.1.45 timezone 6-75
6.1.46 upgrade-status 6-76
6.1.47 version 6-77
6.1.48 wireless 6-78
6.1.49 wwan 6-85

Chapter 7, PROFILES 7-1
7.1 Creating Profiles 7-2
7.1.1 aaa 7-4
7.1.2 arp 7-6
7.1.3 auto-learn-staging-config 7-8
7.1.4 autoinstall 7-9
7.1.5 ap-upgrade 7-10
7.1.6 bridge commands 7-11
7.1.7 cdp 7-21
7.1.8 cluster 7-22
7.1.9 configuration-persistence 7-24
7.1.10 controller 7-25
7.1.11 crypto 7-27
7.1.12 isakmp-policy 7-31
7.1.13 crypto-group 7-38
7.1.14 dscp-mapping 7-41
7.1.15 email-notification 7-42
7.1.16 enforce-version 7-44
7.1.17 events 7-46
7.1.18 ip 7-47

7.1.19 nat-pool 7-51
7.1.20 interface 7-54
7.1.21 Interface Config Instance 7-56
7.1.22 Interface vlan Instance 7-75
7.1.23 led 7-83
7.1.24 legacy-auto-downgrade 7-84
7.1.25 legacy-auto-update 7-85
7.1.26 lldp 7-86
7.1.27 load-balancing 7-87
7.1.28 local 7-89
7.1.29 logging 7-90
7.1.30 mac-address-table 7-92
7.1.31 mint 7-93
7.1.32 misconfiguration-recovery-time 7-96
7.1.33 monitor 7-97
7.1.34 neighbor-inactivity-timeout 7-98
7.1.35 neighbor-info-interval 7-99
7.1.36 no 7-100
7.1.37 noc 7-101
7.1.38 ntp 7-102
7.1.39 preferred-controller-group 7-103
7.1.40 power-config 7-104
7.1.41 radius 7-105
7.1.42 rf-domain-manager 7-106
7.1.43 service 7-107
7.1.44 spanning-tree 7-108
7.1.45 use 7-111
7.1.46 vpn 7-113
7.1.47 wep-shared-key-auth 7-114
7.2 Device Specific Commands 7-115
7.2.1 ap-upgrade 7-117
7.2.2 area 7-118
7.2.3 contact 7-119
7.2.4 country-code 7-120
7.2.5 dhcp-redundancy 7-121
7.2.6 floor 7-122
7.2.7 hostname 7-123
7.2.8 layout-coordinates 7-124
7.2.9 location 7-125
7.2.10 mac-name 7-126
7.2.11 neighbor-info-interval 7-127
7.2.12 override-wlan 7-128
7.2.13 remove-override 7-129
7.2.14 rsa-key 7-130
7.2.15 sensor-server 7-131
7.2.16 stats 7-132
7.2.17 timezone 7-133
7.2.18 trustpoint 7-134
7.2.19 wwan 7-135

Chapter 8, AAA-POLICY 8-1
8.1 aaa-policy 8-2
8.1.1 accounting 8-3
8.1.2 authentication 8-7
8.1.3 mac-address-format 8-11
8.1.4 no 8-12
8.1.5 server-pooling-mode 8-13
8.1.6 use 8-14
8.1.7 write 8-15
8.1.8 clrscr 8-17
8.1.9 commit 8-18
8.1.10 do 8-19
8.1.11 end 8-21
8.1.12 exit 8-22
8.1.13 health-check 8-23
8.1.14 help 8-24
8.1.15 revert 8-25
8.1.16 service 8-26
8.1.17 show 8-28

Chapter 9, AUTO-PROVISIONING-POLICY 9-1
9.1 auto-provisioning-policy 9-2
9.1.1 adopt 9-3
9.1.2 default-adoption 9-6
9.1.3 deny 9-7
9.1.4 no 9-9

Chapter 10, ADVANCED-WIPS-POLICY 10-1
10.1 advanced-wips-policy 10-2
10.1.1 event 10-3
10.1.2 no 10-8
10.1.3 server-listen-port 10-9
10.1.4 terminate 10-10
10.1.5 use 10-11

Chapter 11, ASSOCIATION-ACL-POLICY 11-1
11.1 association-acl-policy 11-2
11.1.1 deny 11-3
11.1.2 no 11-4
11.1.3 permit 11-5

Chapter 12, ACCESS-LIST 12-1
12.1 ip-access-list 12-3
12.1.1 deny 12-4
12.1.2 permit 12-9
12.1.3 no 12-15
12.1.4 write 12-16

12.1.5 clrscr 12-18
12.1.6 commit 12-19
12.1.7 end 12-20
12.1.8 exit 12-21
12.1.9 help 12-22
12.1.10 revert 12-23
12.1.11 service 12-24
12.1.12 show 12-26
12.2 mac-access-list 12-27
12.2.1 permit 12-28
12.2.2 deny 12-35

Chapter 13, DHCP-SERVER-POLICY 13-1
13.1 dhcp-server-policy 13-2
13.1.1 bootp 13-3
13.1.2 dhcp-pool 13-4
13.1.3 dhcp-pool-mode 13-5
13.1.4 static-binding 13-22
13.1.5 static-binding-mode 13-24
13.1.6 option 13-38
13.1.7 no 13-39
13.1.8 ping 13-40
13.1.9 dhcp-class 13-41
13.1.10 dhcp-class-mode 13-42

Chapter 14, FIREWALL-POLICY 14-1
14.1 firewall-policy 14-2
14.1.1 alg 14-3
14.1.2 clamp 14-4
14.1.3 dhcp-offer-convert 14-5
14.1.4 dns-snoop 14-6
14.1.5 firewall 14-7
14.1.6 flow 14-8
14.1.7 ip 14-10
14.1.8 ip-mac 14-14
14.1.9 logging 14-15
14.1.10 no 14-16
14.1.11 proxy-arp 14-17
14.1.12 stateful-packet-inspection-12 14-18
14.1.13 storm-control 14-19
14.1.14 virtual-defragmentation 14-21

Chapter 15, IGMP-SNOOP-POLICY 15-1
15.1 igmp-snoop-policy 15-2
15.1.1 igmp-snooping 15-3
15.1.2 querier 15-4
15.1.3 robustness-variable 15-5
15.1.4 unknown-multicast-fwd 15-6

15.1.5 no 15-7

Chapter 16, MINT-POLICY ----- 16-1
16.1 mint-policy 16-2
16.1.1 level 16-3
16.1.2 mtu 16-4
16.1.3 re-join timeout 16-5
16.1.4 security-level 16-6
16.1.5 sign-unknown-device 16-7
16.1.6 udp 16-8
16.1.7 no 16-9

Chapter 17, MANAGEMENT-POLICY ----- 17-1
17.1 management-policy 17-2
17.1.1 aaa-login 17-3
17.1.2 banner 17-5
17.1.3 ftp 17-6
17.1.4 http 17-8
17.1.5 https 17-9
17.1.6 idle-session-timeout 17-10
17.1.7 no 17-11
17.1.8 restrict-access 17-12
17.1.9 snmp-server 17-13
17.1.10 ssh 17-16
17.1.11 telnet 17-17
17.1.12 user 17-18

Chapter 18, RADIUS-POLICY ----- 18-1
18.1 radius-group 18-2
18.1.1 guest 18-3
18.1.2 policy 18-4
18.1.3 rate-limit 18-7
18.1.4 no 18-8
18.2 radius-server-policy 18-9
18.2.1 authentication 18-10
18.2.2 crl-check 18-11
18.2.3 ldap-group-verification 18-12
18.2.4 ldap-server 18-13
18.2.5 local 18-15
18.2.6 nas 18-16
18.2.7 no 18-17
18.2.8 proxy 18-18
18.2.9 session-resumptionn 18-19
18.2.10 use 18-20
18.3 radius-user-pool-policy 18-21
18.3.1 user 18-22
18.3.2 no 18-23

Chapter 19, RADIO-QOS-POLICY ---------- 19-1
19.1 radio-qos-policy 19-2
19.1.1 accelerated-multicast 19-3
19.1.2 admission-control 19-4
19.1.3 no 19-6
19.1.4 wmm 19-7

Chapter 20, ROLE-POLICY ---------- 20-1
20.1 role-policy 20-2
20.1.1 default-role 20-3
20.1.2 no 20-4
20.1.3 user-role 20-5

Chapter 21, SMART-RF-POLICY ---------- 21-1
21.1 smart-rf-policy 21-2
21.1.1 assignable-power 21-3
21.1.2 auto-assign-sensor 21-4
21.1.3 channel-list 21-5
21.1.4 channel-width 21-6
21.1.5 coverage-hole-recovery 21-7
21.1.6 enable 21-8
21.1.7 group-by 21-9
21.1.8 interference-recovery 21-10
21.1.9 neighbor-recovery 21-11
21.1.10 no 21-12
21.1.11 sensitivity 21-13
21.1.12 smart-ocs-monitoring 21-14

Chapter 22, WIPS-POLICY ---------- 22-1
22.1 wips-policy 22-2
22.1.1 ap-detection 22-3
22.1.2 enable 22-4
22.1.3 event 22-5
22.1.4 history-throttle-duration 22-8
22.1.5 no 22-9
22.1.6 use 22-10
22.1.7 signature 22-11

Chapter 23, WLAN-QOS-POLICY ---------- 23-1
23.1 wlan-qos-policy 23-2
23.1.1 accelerated-multicast 23-3
23.1.2 classification 23-4
23.1.3 multicast-mask 23-6
23.1.4 no 23-7
23.1.5 qos 23-8
23.1.6 rate-limit 23-9
23.1.7 svp-prioritization 23-11

23.1.8 voice-prioritization 23-12
23.1.9 wmm 23-13

Chapter 24, INTERFACE-RADIO COMMANDS 24-1
24.1 interface-radio Instance 24-3
24.1.1 aggregation 24-5
24.1.2 airtime-fairness 24-6
24.1.3 antenna-diversity 24-7
24.1.4 antenna-gain 24-8
24.1.5 antenna-mode 24-9
24.1.6 beacon 24-10
24.1.7 channel 24-11
24.1.8 data-rates 24-12
24.1.9 description 24-15
24.1.10 dynamic-chain-selection 24-16
24.1.11 guard-interval 24-17
24.1.12 lock-rf-mode 24-18
24.1.13 max-clients 24-19
24.1.14 mesh 24-20
24.1.15 no 24-21
24.1.16 non-unicast 24-22
24.1.17 off-channel-scan 24-23
24.1.18 placement 24-24
24.1.19 power 24-25
24.1.20 preamble-short 24-26
24.1.21 probe-response 24-27
24.1.22 radio-share-mode 24-28
24.1.23 rf-mode 24-29
24.1.24 rifs 24-30
24.1.25 rts-threshold 24-31
24.1.26 shutdown 24-32
24.1.27 sniffer-redirect 24-33
24.1.28 use 24-34
24.1.29 wlan 24-35
24.1.30 wireless-client 24-37

Chapter 25, FIREWALL LOGGING 25-1
25.1 Firewall Log Terminology and Syslog Severity Levels 25-2
25.1.1 Date format in Syslog messages 25-3
25.1.2 FTP data connection log 25-4
25.1.3 UDP packets log 25-6
25.1.4 ICMP type logs 25-7
25.1.5 ICMP type logs 25-8
25.1.6 Raw IP Protocol logs 25-9
25.1.7 Raw IP Protocol logs 25-10
25.1.8 Firewall startup log 25-11
25.1.9 Manual time change log 25-12
25.1.10 Firewall ruleset log 25-13
25.1.11 TCP Reset Packets log 25-15

25.1.12 ICMP Destination log 25-16
25.1.13 ICMP Packet log 25-17
25.1.14 SSH connection log 25-18
25.1.15 Allowed/Dropped Packets Log 25-19
26.1 Creating a First Controller Managed WLAN 26-2
26.1.1 Assumptions 26-3
26.1.2 Design 26-4
26.1.3 Using the Command Line Interface to Configure the WLAN 26-5

About This Guide

This guide provides information on using the following Motorola wireless controllers:

- RFS7000
- RFS6000
- RFS4000
- AP7131
- AP650
- AP6511
- AP6532

This document is organized into the following sections:

- *Document Set*
- *Document Convention*
- *Notational Conventions*

Document Set

The documentation set for the Motorola RF Series Controllers is partitioned into the following guides to provide information for specific user deployment requirements.

- **Installation Guides** - Each controller has a unique Installation Guide which describes the basic hardware setup and configuration required to transition to more advanced configuration
- **Motorola RF Series Wireless LAN Controllers WiNG System Reference** - Describes configuration of the Motorola wireless controllers using the Web UI.
- **Motorola RF Series Wireless LAN Controllers WiNG CLI Reference** - Describes the *Command Line Interface* (CLI) and *Management Information Bas*e (MIB) commands used to configure the Motorola wireless controllers.
- **RF Management Software Users Guide** - Describes how to use Motorola RFMS to set up and monitor your wireless controller in respect to areas of good RF throughput and defined physical barriers.

Document Convention

The following conventions are used in this document to draw your attention to important information:

NOTE: Indicates tips or special requirements.

CAUTION: Indicates conditions that can cause equipment damage or data loss.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Switch Note: Indicates caveats unique to a RFS7000, RFS6000 or RFS4000 model controller.

Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents
- Bullets (•) indicate:
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
  - action items
- Sequential lists (those describing step-by-step procedures) appear as numbered lists

Understanding Command Syntax

<variable>	Variables are described with a short description enclosed within a '<' and a '>' pair.
	For example, the command,
	`rfs7000-37FABE>show interface ge 1`
	is documented as
	`show interface ge <idx>`
	• show – The command – Display information
	• interface – The keyword – The interface
	• <idx> – The variable – ge Index value

|	The pipe symbol. This is used to separate the variables/keywords in a list.
	For example, the command
	`rfs7000-37FABE> show .....`
	is documented as
	`show [adoption|advanced-wips|boot|captive-portal|......]`
	where:
	• show – The command
	• [adoption|advanced-wips|boot|captive-portal|.....] – Indicates the different commands that can be combined with the show command. However, only one of the above list can be used at a time.
	`show adoption ...`
	`show advanced-wips ...`
	`show boot ...`

[]	Of the different keywords and variables listed inside a '[' & ']' pair, only one can be used. Each choice in the list is separated with a '|' (pipe) symbol.
	For example, the command
	`rfs7000-37FABE# clear ...`
	is documented as
	`clear [arp-cache|cdp|crypto|event-history| firewall|ip|spanning-tree]`
	where:
	• clear – The command
	• [arp-cache|cdp|crypto|event-history|firewall|ip|spanning-tree] – Indicates that seven keywords are available for this command and only one can be used at a time

{ }	Any command/keyword/variable or a combination of them inside a *'{'* & *'}'* pair is optional. All optional commands follow the same conventions as listed above. However they are displayed italicized.
	For example, the command
	`rfs7000-37FABE> show adoption ....`
	is documented as
	`show adoption info {on <DEVICE-OR-DOMAIN-NAME>}`
	Here:
	• show adoption info – The command. This command can also be used as
	`show adoption info`
	• {on <DEVICE-OR-DOMAIN-NAME>} – The optional keyword *on <device-or-domain-name>*. The command can also be extended as
	`show adoption info {on <DEVICE-OR-DOMAIN-NAME>}`
	Here the keyword *{on <DEVICE-OR-DOMAIN-NAME>}* is optional.

command / keyword	The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.
	For example, the command,
	`rfs7000-37FABE>show wireless`
	is documented as
	`show wireless`
	where:
	• show – The command
	• wireless – The keyword

()	Any command/keyword/variable or a combination of them inside a *'('* & *')'* pair are recursive. All recursive commands can be listed in any order and can be used once along with the rest of the commands.
	For example, the command
	`crypto pki export request generate-rsa-key test autogen-subject-name ...`
	is documented as
	`rfs7000-37FABE#crypto pki export request generate-rsa-key test autogen-subject-name (<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>)`
	Here:
	• crypto pki export request generate-rsa-key <RSA-KEYPAIR-NAME> auto-gen-subject-name – is the command
	`rfs7000-37FABE#crypto pki export request generate-rsa-key test autogen-subject-name`
	• (<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>) – is the set of recursive parameters that can be used in any order.
	where every recursive command is separated by a comma ','.

Motorola Enterprise Mobility Support Center

If you have a problem with your equipment, contact Enterprise Mobility Support for your region.

Contact information is available by visiting *http://www.motorola.com/customersupport* and after selecting your region, click on the appropriate link under Support for Business.

When contacting Enterprise Mobility support, please provide the following information:

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

Motorola responds to calls by email, telephone or fax within the time limits set forth in support agreements. If you purchased your Enterprise Mobility business product from a Motorola business partner, contact that business partner for support.

Customer Support Web Site

Motorola's Support Central Web site, accessed via the Symbol-branded products link under Support for Business, provides information and online assistance including developer tools, software downloads, product manuals and online repair requests

Product Sales and Product Information

Motorola, Inc.

One Motorola Plaza

Holtsville, New York 11742-1300

Tel: 1-631-738-2400 or 1-800-722-6234

Fax: 1-631-738-5990

General Information

For general information, contact Motorola at:

Telephone (North America): 1-800-722-6234

Telephone (International): +1-631-738-5200

Website: *http://www.motorola.com*

Motorola, Inc.
End-User License Agreement

BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE DESCRIBED IN THIS DOCUMENT, YOU OR THE ENTITY OR COMPANY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT ("AGREEMENT"). LICENSEE'S USE OR CONTINUED USE OF THE DOWNLOADED OR INSTALLED MATERIALS SHALL ALSO CONSTITUTE ASSENT TO THE TERMS OF THIS AGREEMENT. IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT CONTINUTE THE INSTALLATION PROCESS. IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO AND EXPRESSLY CONTINGENT UPON THESE TERMS. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF A COMPANY, ANOTHER PERSON OR ANY OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THAT COMPANY, PERSON OR ENTITY.

1. LICENSE GRANT. Subject to the terms of this Agreement, Motorola, Inc. and/or its subsidiaries ("Licensor") hereby grants Licensee a limited, personal, non-sublicensable, non transferable, non-exclusive license to use the software that Licensee is about to download or install and the documentation that accompanies it (collectively, the "Software") for Licensee's personal use in connection with hardware produced by Licensor and only in accordance with the accompanying documentation. Licensee may download, install and use the Software only on a single computer. Licensee may make one copy of the Software (excluding any documentation) for backup purposes, provided that copyright and other restricted rights notices of Licensor and its suppliers are reproduced exactly.
2. LICENSE RESTRICTIONS. Except as expressly permitted by this Agreement, Licensee shall not, nor permit anyone else to, directly or indirectly: (i) copy (except for one backup copy), modify, distribute or create derivative works based upon the Software; (ii) reverse engineer, disassemble, decompile or otherwise attempt to discover the source code or structure, sequence and organization of the Software; or (iii) rent, lease, or use the Software for timesharing or service bureau purposes, or otherwise use the Software for any commercial purpose/on behalf of any third party. Licensee shall maintain and not remove or obscure any proprietary notices on the Software, and shall reproduce such notices exactly on all permitted copies of the Software. All title, ownership rights, and intellectual property rights in and to the Software, and any copies or portions thereof, shall remain in Licensor and its suppliers or licensors. Licensee understands that Licensor may modify or discontinue offering the Software at any time. The Software is protected by the copyright laws of the United States and international copyright treaties. The Software is licensed, not sold. This Agreement does not give Licensee any rights not expressly granted herein.
3. INTELLECTUAL PROPERTY; CONTENT. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Software), and any copies you are permitted to make herein are owned by Licensor or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the Software is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. As a condition to Licensee's use of the Software, Licensee represents, warrants and covenants that Licensee will not use the Software: (i) to infringe the intellectual property rights or proprietary rights, or rights of publicity or privacy, of any third party; (ii) to violate any applicable law, statute, ordinance or regulation; (iii) to disseminate information or materials in any form or format ("Content") that are harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, or otherwise objectionable; or (iv) to disseminate any software viruses or any other computer code, files or programs that may interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment. Licensee, not Licensor, remains solely responsible for all Content that Licensee uploads, posts, e-mails, transmits, or otherwise disseminates using, or in connection with, the Software.
4. FEES; SUPPORT AND UPGRADES. Licensor may, at Licensor's sole option, provide support services related to the Software ("Support Services"). Nothing in this Agreement grants Licensee any right to receive any Support Services. Use of any Support Services provided is governed by the Licensor policies and programs described in the user manual, in "online" documentation, and/or in other Licensor-provided materials or support agreements. Any supplemental software code provided to you as part of any Support Services shall be considered part of the Software and subject to the terms and conditions of this EULA. With respect to technical information you provide to Licensor as part of any Support Services,

Licensor may use such information for its business purposes, including for product support and development. Licensor will not utilize such technical information in a form that personally identifies Licensee.

5. TERMINATION. Either party may terminate this Agreement at any time, with or without cause, upon written notice. Any termination of this Agreement shall also terminate the licenses granted hereunder. Upon termination of this Agreement for any reason, Licensee shall return all copies of the Software to Licensor, or destroy and remove from all computers, hard drives, networks, and other storage media all copies of the Software, and shall so certify to Licensor that such actions have occurred. Sections 2-13 shall survive termination of this Agreement.
6. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, Licensor and its suppliers provide the Software and any (if any) Support Services AS IS AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability, of fitness for a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of workmanlike effort, all with regard to the Software, and the provision of or failure to provide Support Services. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NONINFRINGEMENT WITH REGARD TO THE SOFTWARE. THE ENTIRE RISK AS TO THE QUALITY OF OR ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE AND SUPPORT SERVICES, IF ANY, REMAINS WITH LICENSEE.
7. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR OR ITS SUPPLIERS BE LIABLE FOR ANY GENERAL, SPECIAL, INCIDENTAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF LICENSOR OR ANY SUPPLIER, AND EVEN IF LICENSOR OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
8. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that Licensee might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of Licensor and any of its suppliers under any provision of this Agreement and Licensee's exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by Licensee for the Software or U.S.$5.00. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

9. INDEMNITY. Licensee agrees that Licensor shall have no liability whatsoever for any use Licensee makes of the Software. Licensee shall indemnify and hold harmless Licensor from any claims, damages, liabilities, costs and fees (including reasonable attorney fees) arising from Licensee's use of the Software as well as from Licensee's failure to comply with any term of this Agreement.
10. FAULT TOLERANCE. The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale in on-line control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to, the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, life support machines, or weapons systems, in which the failure of the Software could lead directly or indirectly to death, personal injury, or physical or environmental damage ("High Risk Activities"). Licensor and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.
11. U.S. GOVERNMENT LICENSE RIGHTS. Software provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described elsewhere herein. Software provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227- 7013 (OCT 1988), as applicable. The "Manufacturer" for purposes of these regulations is Motorola, Inc., One Symbol Plaza, Holtsville, NY 11742.
12. EXPORT RESTRICTIONS. Licensee shall comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and Licensee shall not export, or allow the export or re-export of the Software in violation of any such restrictions, laws or regulations. By downloading or using the Software, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any restricted country.
13. MISCELLANEOUS. Licensee may not sublicense, assign, or transfer this Agreement, or its rights or obligations hereunder, without the prior written consent of Licensor. Any attempt to otherwise sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is null and void. Licensor may assign this Agreement in its sole discretion. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be illegal, invalid or unenforceable, such provisions shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect. No waiver or modification of this Agreement will be binding upon a party unless made in writing and signed by a duly authorized representative of such party and no failure or delay in enforcing any right will be deemed a waiver. This Agreement shall be governed by the laws of the State of New York without regard to the conflicts of law provisions thereof. The application the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Unless waived by Licensor for a particular instance, any action or proceeding arising out of this Agreement must be brought exclusively in the state or federal courts of New York and Licensee hereby consents to the jurisdiction of such courts for any such action or proceeding. This Agreement supersedes all prior discussions and writings and constitutes the entire agreement between the parties with respect to the subject matter hereof. The prevailing party in any action arising out of this Agreement shall be entitled to costs and attorneys' fees.

CHAPTER 1 INTRODUCTION

This chapter describes the commands available using the controller *Command Line Interface* (CLI) on a Motorola Solutions device. CLI is available for all supported devices, controllers as well as *Access Points* (APs).

Access the CLI by:

- A terminal emulation program running on a computer connected to the serial port on the controller. The serial port is located on the front of the controller.
- A Telnet session through *Secure Shell* (SSH) over a network.

Configuration for connecting to a Controller using a terminal emulator

If connecting through the serial port, use the following settings to configure your terminal emulator:

Bits Per Second	19200
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	None

When a CLI session is established, complete the following (user input is in **bold**):

```
login as: <username>
administrator's login password: <password>
```

User Credentials

Use the following credentials when logging into a device for the first time:

User Name	admin
Password	motorola

When logging into the CLI for the first time, you are prompted to change the password.

Examples in this reference guide

Examples used in this reference guide are generic to the each supported controller model and AP. Commands that are not common, are identified using the notation "Supported in the following platforms." For an example, see below:

Supported in the following platforms:

- *RFS6000*

The above example indicates the command is only available on a RFS6000 model controller.

1.1 CLI Overview

The CLI is used for configuring, monitoring, and maintaining the controller managed network. The user interface allows you to execute commands on supported controllers and AP models, using either a serial console or a remote access method.

This chapter describes basic CLI features. Topics covered include an introduction to command modes, navigation and editing features, help features and command history.

The CLI is segregated into different command modes. Each mode has its own set of commands for configuration, maintenance and monitoring. The commands available at any given time depend on the mode you are in, and to a lesser extent, the particular model used. Enter a question mark (?) at the system prompt to view a list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is: USER EXEC mode, PRIV EXEC mode and GLOBAL CONFIG mode.

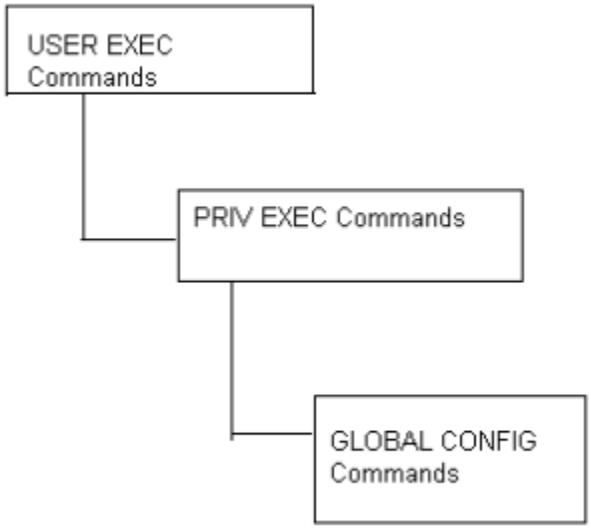

Figure 1-1 *Hierarchy of User Modes*

Command Modes

A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is reserved for tasks that do not change the controller configuration.

```
rfs7000-37FABE>
```

The system prompt signifies the device name and the last three bytes of the device MAC address.

To access commands, enter the PRIV EXEC mode (the second access level for the EXEC mode). Once in the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

```
rfs7000-37FABE> enable
rfs7000-37FABE#
```

Most of the USER EXEC mode commands are one-time commands and are not saved across controller reboots. Save the command by executing 'commit' command. For example, the show command displays the current configuration and the clear command clears the interface.

Access the GLOBAL CONFIG mode from the PRIV EXEC mode. In the GLOBAL CONFIG mode, enter commands that set general system characteristics. Configuration modes, allow you to change the running configuration. If you save the configuration later, these commands are stored across controller reboots.

Access a variety of protocol specific (or feature-specific) modes from the global configuration mode. The CLI hierarchy requires you to access specific configuration modes only through the global configuration mode.

```
rfs7000-37FABE# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs7000-37FABE(config)#
```

You can also access sub-modes from the global configuration mode. Configuration sub-modes define specific features within the context of a configuration mode.

```
rfs7000-37FABE(config)# aaa-policy test
rfs7000-37FABE(config-aaa-policy-test)#
```

Table 1.1 Summarizes available controller commands.

Table 1.1 *All Modes Commands*

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
ap-upgrade	ap-upgrade	aaa-policy
change-passwd	archive	advanced-wips-policy
clear	boot	ap650
clock	cd	ap6511
cluster	change-passwd	ap6532
commit	clear	ap71xx
connect	clock	association-acl-policy
crypto	cluster	auto-provisioning-policy
debug	commit	captive-portal
disable	configure	clear
enable	connect	critical-resource-policy
help	copy	customize
logging	crypto	device
mint	debug	device-categorization
no	delete	dhcp-server-policy
page	diff	dns-whitelist
ping	dir	event-system-policy
remote-debug	disable	firewall-policy
revert	edit	help
service	enable	host
show	erase	igmp-snoop-policy

Table 1.1 *All Modes Commands*

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
telnet	format	ip
terminal	halt	mac
time-it	help	management-policy
traceroute	logging	mint-policy
watch	mint	nac-list
write	mkdir	no
clrscr	more	password-encryption
exit	no	profile
	page	radio-qos-policy
	ping	radius-group
	pwd	radius-server-policy
	reload	radius-user-pool-policy
	remote-debug	rf-domain
	rename	rfs4000
	revert	rfs6000
	rmdir	rfs7000
	self	role-policy
	service	self
	show	smart-rf-policy
	telnet	wips-policy
	terminal	wlan
	time-it	wlan-qos-policy
	traceroute	write
	upgrade	clrscr
	upgrade-abort	commit
	watch	do
	write	end
	clrscr	exit
	exit	revert

Table 1.1 *All Modes Commands*

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
		service
		show

1.2 Getting Context Sensitive Help

Enter a question mark (?) at the system prompt to display a list of commands available for each mode. Obtain a list of arguments and keywords for any command using the CLI context-sensitive help.

Use the following commands to obtain help specific to a command mode, command name, keyword or argument:

Command	***Description***
(prompt)# help	Displays a brief description of the help system
(prompt)# abbreviated-command-entry?	Lists commands in the current mode that begin with a particular character string
(prompt)# abbreviated-command-entry<Tab>	Completes a partial command name
(prompt)# ?	Lists all commands available in the command mode
(prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command
(prompt)# command keyword ?	Lists the next available syntax option for the command

NOTE: The system prompt varies depending on which configuration mode your in.

NOTE: Enter Ctrl + V to use ? as a regular character and not as a character used for displaying context sensitive help. This is required when the user has to enter a URL that ends with a ?

NOTE: The escape character used through out the CLI is "\". To enter a "\" use "\\" instead.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular sequence, enter the characters followed by a question mark (?). Do not include a space. This form of help is called word help, because it completes a word.-

```
rfs7000-37FABE#service?
service Service Commands
rfs7000-37FABE#service
```

Enter a question mark (?) (in place of a keyword or argument) to list keywords or arguments. Include a space before the ?. This form of help is called command syntax help. It shows the keywords or arguments available based on the command/keyword and argument already entered.

```
rfs7000-37FABE>service ?
  advanced-wips      Advanced WIPS service commands
  clear              Clear
  cli-tables-expand  Expand the cli-table in drapdown format
  cli-tables-skin    Choose a formatting layout/skin for CLI tabular outputs
  cluster            Cluster Protocol
```

```
  locator             Enable leds flashing on the device
  pktcap              Start packet capture
  radio               Radio parameters
  show                Show running system information
  smart-rf            Smart-RF Management Commands
  traceroute          Trace route to destination
  wireless            Wireless commands
rfs7000-37FABE>service
```

It's possible to abbreviate commands and keywords to allow a unique abbreviation. For example, "configure terminal" can be abbreviated as **`config t`**. Since the abbreviated command is unique, the controller accepts the abbreviation and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
rfs7000-37FABE>help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered and you want to
know what arguments match the input
   (e.g. 'show ve?'.)
```

1.3 Using the No Command

Almost every command has a **no** form. Use no to disable a feature or function or return it to its default value. Use the command without the **no** keyword to re-enable a disabled feature.

1.3.1 Basic Conventions

Keep the following conventions in mind while working within the controller CLI:

- Use ? at the end of a command to display available sub-modes. Type the first few characters of the sub-mode and press the tab key to add the sub-mode. Continue using ? until you reach the last sub-mode.
- Pre-defined CLI commands and keywords are case-insensitive: cfg = Cfg = CFG. However (for clarity), CLI commands and keywords are displayed (in this guide) using mixed case. For example, apPolicy, trapHosts, channelInfo.
- Enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive.

1.4 Using CLI Editing Features and Shortcuts

A variety of shortcuts and edit features are available. The following describe these features:

- *Moving the Cursor on the Command Line*
- *Completing a Partial Command Name*
- *Command Output pagination*

1.4.1 Moving the Cursor on the Command Line

Table 1.2 on page 1-11

Shows the key combinations or sequences to move the command line cursor. Ctrl defines the control key, which must be pressed simultaneously with its associated letter key. Esc means the escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters are used to provide an easy way of remembering their functions. In Table 1.2 on page 1-11, bold characters indicate the relation between a letter and its function.

Table 1.2 *Keystrokes Details*

Keystrokes	***Function Summary***	***Function Details***
Left Arrow or Ctrl-B	Back character	Moves the cursor one character to the left When entering a command that extends beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to move back to the system prompt.
Right Arrow or Ctrl-F	Forward character	Moves the cursor one character to the right
Esc- B	Back word	Moves the cursor back one word
Esc- F	Forward word	Moves the cursor forward one word
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the command line
Ctrl-E	End of line	Moves the cursor to the end of the command line
Ctrl-D		Deletes the current character
Ctrl-U		Deletes text up to cursor
Ctrl-K		Deletes from the cursor to end of the line
Ctrl-P		Obtains the prior command from memory
Ctrl-N		Obtains the next command from memory
Esc-C		Converts the letter at the cursor to uppercase
Esc-L		Converts the letter at the cursor to lowercase
Esc-D		Deletes the remainder of a word
Ctrl-W		Deletes the word up to the cursor
Ctrl-Z		Returns to the root prompt
Ctrl-T		Transposes the character to the left of the cursor with the character located at the cursor.
Ctrl-L		Clears the screen

1.4.2 Completing a Partial Command Name

If you cannot remember a command name (or if you want to reduce the amount of typing you have to perform), enter the first few letters of a command, then press the Tab key. The command line parser completes the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-L.

The CLI recognizes a command once you have entered enough characters to make the command unique. If you enter "conf" within the privileged EXEC mode, the CLI associates the entry with the configure command, since only the configure command begins with **conf**.

In the following example, the CLI recognizes a unique string in the privileged EXEC mode when the Tab key is pressed:

```
rfs7000-37FABE# conf<Tab>
rfs7000-37FABE# configure
```

When using the command completion feature, the CLI displays the full command name. The command is not executed until the Return or Enter key is pressed. Modify the command if the full command was not what you intended in the abbreviation. If entering a set of characters (indicating more than one command), the system lists all commands beginning with that set of characters.

Enter a question mark (?) to obtain a list of commands beginning with that set of characters. Do not leave a space between the last letter and the question mark (?).

For example, entering U lists all commands available in the current command mode:

```
rfs7000-37FABE# co?
 commit     Commit all changes made in this session
  configure  Enter configuration mode
  connect    Open a console connection to a remote device
  copy       Copy from one file to another
rfs7000-37FABE# co
```

NOTE: The characters entered before the question mark are reprinted to the screen to complete the command entry.

1.4.3 Command Output pagination

Output often extends beyond the visible screen length. For cases where output continues beyond the screen, the output is paused and a

```
--More--
```

prompt displays at the bottom of the screen. To resume the output, press the Enter key to scroll down one line or press the Spacebar to display the next full screen of output.

1.4.4 Creating Profiles

Profiles are sort of a 'template' representation of configuration. The system has a couple of default profiles including

- a default controller profile
- a default ap7131 profile

To modify the default controller profile to assign an IP address to the management port:

```
rfs7000-37FABE(config)#profile rfs7000 default-rfs-7000
rfs7000-37FABE(config-profile-default-rfs-7000)#interface me1
rfs7000-37FABE(config-profile-default-rfs-7000-if-me1)#ip address 172.16.10.2/24
rfs7000-37FABE(config-profile-default-rfs-7000-if-me1)#commit
rfs7000-37FABE(config-profile-default-rfs-7000)#exit
rfs7000-37FABE(config)#
The following command displays default ap7131 profile:
rfs7000-37FABE(config)#profile ap7131 default-ap7131
```

```
rfs7000-37FABE(config-profile-default-ap7131)#show context
```

1.4.5 Change the default profile by creating vlan 150 and mapping to ge3 Physical interface

Logon to the controller in config mode and follow the procedure below:

```
rfs7000-37FABE(config-profile-default-rfs7000)# interface vlan 150
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan150)# ip address
192.168.150.20/24
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan150)# exit
rfs7000-37FABE(config-profile-default-rfs7000)# interface ge 3
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)# switchport access vlan 150
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)# commit write
[OK]
rfs7000-37FABE(config-profile-default-rfs7000-if-ge3)# show interface vlan 150
Interface vlan150 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 8, Metric: 1, MTU: 1500
  IP-Address: 192.168.150.20/24
    input packets 43, bytes 12828, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

1.4.5.1 Viewing Configured APs

To view previously configured APs, enter the following command:

```
rfs7000-37FABE(config)#show wireless ap configured
```

1.4.6 *Remote Administration*

A terminal server may function in remote administration mode if either the terminal services role is not installed on the machine or the client used to invoke the session has enabled the admin controller.

- A terminal emulation program running on a computer connected to the serial port on the controller. The serial port is located on the front of the controller.
- A Telnet session through a *Secure Shell* (SSH) over a network. The telnet session may or may not use SSH depending on how the wireless controller is configured. Motorola Solutions recommends using SSH for remote administration tasks.

1.4.6.1 Configuring telnet for Management Access

Login through the serial console. Perform the following:

1. A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode).
2. Access the GLOBAL CONFIG mode from the PRIV EXEC mode

   ```
   rfs7000-37FABE> en
   rfs7000-37FABE# configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   ```

3. Go to 'default-management-policy' mode.

   ```
   rfs7000-37FABE(config)# management-policy ?
   rfs7000-37FABE(config)# management-policy default
   rfs7000-37FABE(config-management-policy-default)#
   ```

4. Enter Telnet and the port number at the command prompt. The port number is optional. The default port is 23. Commit the changes after every command. Telnet is enabled.

   ```
   rfs7000-37FABE(config-management-policy-default)# telnet
   rfs7000-37FABE(config-management-policy-default)# commit write
   ```

5. Connect to the wireless controller through telnet using its configured IP address. Use the following credentials when logging on to the device for the first time.

User Name	admin
Password	motorola

When logging into the controller for the first time, you are prompted to change the password.

To change user credentials, perform the following:

1. Enter the username, password, role and access details

```
rfs7000-37FABE(config-management-policy-default)# user testuser password symbol
role helpdesk access all
rfs7000-37FABE(config-management-policy-default)# commit
rfs7000-37FABE(config-management-policy-default)# show context
management-policy default
 telnet
 http server
 ssh
 user admin password 1
c9745a77bb8663fbe9422c0bab93087208e68c40add8edd0a3b4a985aa96a682 role superuser
access all
 user testuser password 1
fd6af6a0e74ede3fc4bd54519e4864b078554aa2d97a623eedefae2ede682c13 role helpdesk
access all
rfs7000-37FABE(config-management-policy-default)# show context include-factory
management-policy default
 secure-management
 telnet port 23
 http server
 no https server
 no ftp
 ssh port 22
 user admin password 1
c9745a77bb8663fbe9422c0bab93087208e68c40add8edd0a3b4a985aa96a682 role superuser
access all
 user testuser password 1
fd6af6a0e74ede3fc4bd54519e4864b078554aa2d97a623eedefae2ede682c13 role helpdesk
access all
 snmp-server manager v2
 snmp-server manager v3
 no snmp-server enable traps
rfs7000-37FABE(config-management-policy-default)#
rfs7000-37FABE(config-management-policy-default)# user testuser password symbol
role helpdesk access all ?
```

2. Logon to the Telnet console and provide the user details configured in the previous step to access the controller.

```
RFS7000 release 5.01.0.0-070D
rfs7000-37FABE login: testuser
Password:
Welcome to CLI
Starting CLI...

rfs7000-37FABE>
```

1.4.6.2 Configuring ssh

By default, SSH is enabled from the factory settings on the controller. The controller requires an IP address and login credentials.

To enable SSH access in the default profile, login through the serial console. Perform the following steps:

1. Access the GLOBAL CONFIG mode from the PRIV EXEC mode

```
rfs7000-37FABE> en
```

```
rfs7000-37FABE# configure
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
rfs7000-37FABE> en
```

```
rfs7000-37FABE# configure
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Go to 'default-management-policy' mode.

```
rfs7000-37FABE(config)# management-policy default
rfs7000-37FABE(config-management-policy-default)#
```

3. Enter SSH at the command prompt.

```
rfs7000-37FABE(config-management-policy-default)# ssh
```

4. Log into the wireless controller through SSH using appropriate credentials.
5. Use the following credentials when logging on to the device for the first time

User Name	admin
Password	motorola

On logging into the controller for the first time, you are prompted to change the password.

- To change the user credentials, perform the following steps:

```
RFS7000 release 5.1.0.0-070D
rfs7000-37FABE login: testuser
Password:
Welcome to CLI
Starting CLI...
```

```
rfs7000-37FABE>
```

CHAPTER 2 USER EXEC MODE COMMANDS

Logging in to the controller places you within the USER EXEC command mode. Typically, a login requires a user name and password. You have three login attempts before the connection attempt is refused. USER EXEC commands (available at the user level) are a subset of the commands available at the privileged level. In general, USER EXEC commands allow you to connect to remote devices, perform basic tests and list system information.

To list available USER EXEC commands, use**?** at the command prompt. The USER EXEC prompt consists of the device host name followed by an angle bracket (**>**).

```
rfs7000-37FABE>?
User Exec commands:
  ap-upgrade      AP firmware upgrade
  change-passwd   Change password
  clear           Clear
  clock           Configure software system clock
  cluster         Cluster commands
  commit          Commit all changes made in this session
  connect         Open a console connection to a remote device
  crypto          Encryption related commands
  debug           Debugging functions
  disable         Turn off privileged mode command
  enable          Turn on privileged mode command
  help            Description of the interactive help system
  logging         Modify message logging facilities
  mint            MiNT protocol
  no              Negate a command or set its defaultsspo
  page            Toggle paging
  ping            Send ICMP echo messages
  remote-debug    Troubleshoot remote system(s)
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  telnet          Open a telnet connection
  terminal        Set terminal line parameters
  time-it         Check how long a particular command took between request and
                  completion of response
  traceroute      Trace route to destination
  watch           Repeat the specific CLI command at a periodic interval
  write           Write running configuration to memory or terminal

  clrscr          Clears the display screen
  exit            Exit from the CLI

rfs7000-37FABE>
```

2.1 User Exec Commands

Table 2.1 Summarizes User Exec Mode Commands

Table 2.1 *User Exec Commands*

Command	Description	Reference
ap-upgrade	Enables an automatic adopted AP firmware upgrade	*page 2-4*
change-passwd	Changes the password of a logged user	*page 2-7*
clear	Resets the last saved command	*page 2-8*
clock	Configures the system clock	*page 2-11*
clrscr	Clears the screen	*page 2-12*
cluster	Accesses the cluster context	*page 2-13*
commit	Commits all the updates in the active session	*page 2-14*
connect	Establishes a console connection to a remote device	*page 2-15*
crypto	Enables encryption	*page 2-16*
disable	Turns off (disables) the privileged mode command set	*page 2-25*
enable	Turns on (enables) the privileged mode command set	*page 2-26*
exit	Ends the current mode and moves to the previous mode	*page 2-27*
help	Displays the interactive help system	*page 2-28*
logging	Modifies message logging facilities	*page 2-32*
mint	Configures the MiNT protocol	*page 2-33*
no	Negates a command or sets its default value	*page 2-35*
page	Toggles to the controller paging function	*page 2-36*
ping	Sends ICMP echo messages to a user-specified location	*page 2-37*
revert	Reverts the changes made in the active session to their last configuration	*page 2-38*
show	Displays the settings for the specified system component	*page 2-40*
telnet	Opens a telnet session	*page 2-42*
terminal	Sets the length/number of lines displayed within the terminal window	*page 2-43*
time-it	Verifies the time taken by a particular command between request and response	*page 2-44*
traceroute	Traces the route to its defined destination	*page 2-45*

Table 2.1 *User Exec Commands*

Command	***Description***	***Reference***
watch	Repeats the specific CLI command at a periodic interval	*page 2-46*
write	Writes the system running configuration to memory or terminal	*page 2-47*

2.1.1 ap-upgrade

User Exec Commands

Enables an automatic adopted AP firmware upgrade

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap-upgrade [<DEVICE-NAME>|all|ap650|ap6511|ap6532|ap71xx|cancel-upgrade|
   load-image|rf-domain]
ap-upgrade [<DEVICE-NAME>|ap650|ap6511|ap6532|ap71xx] all {no-reboot|
   reboot-time <TIME>|upgrade-time <TIME>}]
ap-upgrade all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>}
ap-upgrade cancel-upgrade [<DEVICE-NAME>|ap650|ap6511|ap6532|ap71xx] all
ap-upgrade cancel-upgrade all
ap-upgrade cancel-upgrade on rf-domain [<RF-DOMAINNAME>|all]
ap-upgrade load-image [ap650|ap6511|ap6532|ap71xx] <URL>

ap-upgrade rf-domain <rf-domainname> [all|ap650|ap6511|ap6532|
   ap71xx] {no-reboot|no-via-rf-domain|reboot-time <TIME>|
   upgrade-time <TIME>}
ap-upgrade rf-domain all [all|ap650|ap6511|ap6532|ap71xx]
   {no-reboot|no-via-rf-domain|reboot-time <TIME>|upgrade-time <TIME>}
```

Parameters

[<DEVICE-NAME>|all|ap650 |ap71xx|ap6511|ap6532|] [cancel-upgrade|load-image| rf-domain]	• <DEVICE-NAME> all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Specify the name/MAC address of an AP • all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades all the access points • ap650 all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades an AP650 device • ap6511 all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades an AP6511 device • ap6532 all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades an AP6532 device • ap71xx all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades an AP71xx device • cancel-upgrade [<DEVICE-NAME>|ap650|ap6532|ap71xx| ap6511|all] – Cancels upgrading the AP • load-image [ap650|ap71xx|ap6511] <URL> – Loads the AP firmware images on the Controller • <URL> – Specify the location of firmware image URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • rf-domain <RF-DOMAINNAME> {no-reboot|no-via-rf-domain|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades all the access points belonging to an RF Domain • no-via-rf-domain – Upgrades APs from the adopted device The following are common for all the above: • no-reboot – No reboot (manually reboot after the upgrade) • reboot-time <TIME> – Sets the scheduled reboot time • upgrade-time <TIME> – Sets the scheduled upgrade time • <TIME> – Specify the reboot time in MM/DD/YYYY-HH:MM or HH:MM format

Example

```
rfs7000-37FABE>ap-upgrade ap650 00-A0-F8-00-00-00
rfs7000-37FABE>
rfs7000-37FABE>ap-upgrade all
rfs7000-37FABE>
rfs4000-880DA7>ap-upgrade  default/rfs4000-880DA7 no-reboot
-------------------------------------------------------------------------
CONTROLLER                STATUS                    MESSAGE
-------------------------------------------------------------------------
00-23-68-88-0D-A7          Success          Queued 0 APs to upgrade
-------------------------------------------------------------------------
rfs4000-880DA7>
rfs7000-37FABE#ap-upgrade rfs7000-37FABE reboot-time 06/01/2011-12:10
```

```
-------------------------------------------------------------------------
CONTROLLER              STATUS                    MESSAGE
-------------------------------------------------------------------------
00-15-70-37-FA-BE       Success          Queued 0 APs to upgrade
-------------------------------------------------------------------------
rfs7000-37FABE#
```

2.1.2 change-passwd

User Exec Commands

Changes the password of the logged in user

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`change-passwd {<OLD-PASSWD> <NEW-PASSWD>}`

Parameters

{<OLD-PASSWD> <NEW-PASSWD>}	Optional. The passwords can also be changed interactively. To do so, press Enter after the **change-passwd** command. • <OLD-PASSWD> – The password that needs to be changed • <NEW-PASSWD> – The password to change to.

Usage Guidelines

A password must be between 8 to 32 characters in length.

Example

```
rfs7000-37FABE>change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
rfs7000-37FABE>write memory
OK
rfs7000-37FABE>
```

2.1.3 clear

User Exec Commands

Clears parameters, cache entries, table entries, and other similar entries. The clear command is only available for specific commands. The information cleared using this command varies depending on the mode where the clear command is executed.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

NOTE: Refer to the interface details below when using `clear`

- ge <index> – RFS4000 supports 4GEs and RFS6000 supports 8 GEs
- me1 – Available in both RFS7000 and RFS6000

Syntax

```
clear [arp-cache|cdp|crypto|event-history|ip|lldp|spanning-tree]
clear arp-cache {on <DEVICE-NAME>}
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
clear crypto [ipsec|isakmp] sa [<IP>|all] {on <DEVICE-NAME>}
clear event-history
clear ip dhcp bindings [<A.B.C.D>|all] {on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface {<INTERFACE>|ge <1-8>|me1|port-
channel <1-4>|vlan <1-4094>} {on <DEVICE-NAME>}
```

Parameters

arp-cache *{on <DEVICE--NAME>}*	Clears ARP cache entries. • on <DEVICE-NAME> – Optional. Clears the arp cache on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name
[cdp|lldp] neighbors *{on <DEVICE-NAME>}*	Clears Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) neighbor table entries • neighbors – Clears CDP neighbor table • on <DEVICE-NAME> – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name
crypto [ipsec|isakmp] sa [<IP>|all] {on <DEVICE-NAME>}	Clears the encryption module's databases. • ipsec sa – Clears IPSEC security associations. • isakmp sa – Clears ISAKMP security associations. The following are common for the above: • <IP> – Clears the IPSec or ISAKMP security associations for a certain Peer. • all – Clears the IPSec or ISAKMP security associations for all Peers. • on <DEVICE-NAME> – Optional. Clears the SAs on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name
event-history	Clears event history
ip dhcp bindings [<IP|all] *{on <DEVICE-NAME>}*	Clears the DHCP address bindings. • on <DEVICE-NAME> – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name
spanning-tree detected-protocols {interface {<INTERFACE>|ge <1-8>|me1|port-channel <1-4>|vlan <1-4094>} {on <DEVICE-NAME>}	Clears the spanning-tree protocols configured for the interface • detected-protocols *{interface [<INTERFACE>|ge <1-8>|me1|port-channel <1-4>|vlan <1-4094>]} {on}* – Enter the interface name to clear the detected spanning tree protocols for that specific interface • <INTERFACE> – Clears selected interface name • ge < 1-8> – Clears the configured GigabitEthernet interface status • me1 – Clears the FastEthernet interface status • port-channel <1-4> – Clears port-channel information on AP/Controller • vlan <1-4094> – Clears the configured vlan information • wwan1 – Clears Wireless WAN interface information The following are common for the above • on <DEVICE-NAME> – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name

Example

```
rfs7000-37FABE>clear crypto isakmp sa 111.222.333.01 on rfs7000-37FABE
```

```
rfs7000-37FABE>

rfs7000-37FABE>clear event-history
rfs7000-37FABE>

rfs7000-37FABE>clear spanning-tree detected-protocols interface port-channel 1 on
rfs7000-37FABE
rfs7000-37FABE>

rfs7000-37FABE>clear ip dhcp bindings 172.16.10.9 on rfs7000-37FABE
rfs7000-37FABE>

rfs7000-37FABE#clear cdp neighbors on rfs7000-37FABE
rfs7000-37FABE#
rfs4000-880DA7#clear spanning-tree detected-protocols interface ge 1
rfs4000-880DA7#

rfs4000-880DA7#clear lldp neighbors
rfs4000-880DA7#
```

2.1.4 clock

User Exec Commands

Configures the system clock

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

Parameters

set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}	• Sets the software system clock for the configured device • <HH:MM:SS> – Sets the current time (in military format hours, minutes and seconds) • <1-31> – Enter the numerical day of the month • <MONTH> – Enter the month of the year (Jan to Dec) • <1993-2035> – Select a valid digit year from 1993-2035 • on – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE>clock set 12:30:45 2 MONTH 2010 on rfs7000-37FABE
clock set 12:30:45 2 MONTH 2010 on rfs7000-37FABE rfs7000-37FABE>
```

2.1.5 clrscr

User Exec Commands

Clears the screen and refreshes the prompt (**#**)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clrscr
```

Parameters

None

Example

```
rfs7000-37FABE>clrscr
rfs7000-37FABE>
```

2.1.6 cluster

User Exec Commands

Use this command to initiate the cluster context. The cluster context provides centralized management to configure all the cluster members from any one member.

Commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
cluster start-selection
```

Parameters

start-selection	Starts a new cluster master election

Example

```
rfs7000-37FABE>cluster start-election
rfs7000-37FABE>
```

2.1.7 commit

User Exec Commands

Commits all the changes made in the active session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
commit {write memory}
```

Parameters

write memory	If a commit succeeds, the configuration is written to memory • memory – Writes the changes to memory

Example

```
rfs7000-37FABE>commit write memory
[OK]
rfs7000-37FABE>
```

2.1.8 connect

User Exec Commands

Begins a console connection to a remote device using the remote device's MINT ID or its device name.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

Parameters

mint-id <MINT-ID>	Connects to the remote system using MINT ID. • <MINT-ID> – The MINT Id of the remote device.
<REMOTE-DEVICE-NAME>	Connects to the remote system using its device name.

Example

```
rfs7000-37FABE#connect  RFDOMAIN_UseCase1/rfs7000-37FAAA

Entering character mode
Escape character is '^]'.
RFS7000 release 5.0.0.0-061D
rfs7000-37FABE login: admin
Password:
Welcome to CLI
rfs7000-37FAAA>
```

2.1.9 crypto

User Exec Commands

Enables encryption

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
crypto [key|pki]

crypto key [export|generate|import|zeroise]
crypto key export rsa <RSA-KEYPAIR-NAME>> <EXPORT-TO-URL>
   {background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
    {background} {on <DEVICE-NAME>}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {passphrase <KEY-
PASSPHRASE>} {background} {on <DEVICE-NAME>}

crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048>
   {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
    {background} {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> passphrase <KEY-
PASSPHRASE> {background} {on <DEVICE-NAME>}

crypto key  zeroise rsa <RSA-KEYPAIR-NAME> {force} {on <DEVICE-NAME>}

crypto pki [authenticate|export|generate|import|zeroise]
crypto pki authenticate <TRUST-POINT> <URL> {background} {on <DEVICE-NAME>}

crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|use-rsa-key]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-
subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-
subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)

crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-
subject-name <EXPORT-TO-URL> {background} {on <DEVICE-NAME>}

crypto pki export request [generate-rsa-key|use-rsa-key] <WORD> subject-name <COMMON-
NAME> <COUNTRY>  <STATE> <CITY> <ORGANISATION> <ORGANIZATION-UNIT> [<EXPORT-TO-
URL>|email <SEND-TO-EMAIL>|fqdn <FQDN>|ip-address <IP>]

crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {{background} {on
<DEVICE--NAME>}|passphrase <KEY-PHRASE> {background} {on <DEVICE-NAME>}|on <DEVICE-
NAME>}}

crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> [autogen-subject-name|subject-name]

crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name {email|fqdn|ip-address|on}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name email <WORD> {fqdn <WORD>|ip-address <A.B.C.D>|on
<DEVICE-NAME>}
crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name fqdn <WORD> {email <WORD>|ip-address <A.B.C.D>|on
<DEVICE-NAME>}
crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name ip-address <A.B.C.D> {fqdn <WORD>|on <DEVICE-NAME>}
crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name {on <DEVICE-NAME>}

crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> subject-name <COMMON-NAME> <COUNTRY>  <STATE> <CITY> <ORGANISATION>
<ORGANIZATION-UNIT> {email <WORD>|fqdn <WORD>|ip-address <A.B.C.D>|on} <DEVICE-NAME>

crypto pki import [certificate|crl|trustpoint]
crypto pki import [certificate|crl] <WORD> <IMPORT-FROM-URL> {background {on <DEVICE-
NAME>}|on <DEVICE--NAME>}]

crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background {on
<DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <word> {background {on <DEVICE-NAME>}|on
<DEVICE-OR-DOMAIN-NAME>}

crypto pki zeroise trustpoint <TRUSTPOINT-NAME> {del-key {on
<DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-NAME>}
```

Parameters

key	Performs key management operations
key export	• export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background|on|phrase} – Performs export operation • rsa <RSA-KEYPAIR-NAME> – Enter the name of a RSA keypair to export • <EXPORT-TO-URL> {background|on|phrase} – Enter the location to send the key using the following syntax: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • background {on <DEVICE-NAME>} – Performs the operation in background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • passphrase <KEY-PASSPHRASE> {background|on} – Enter a passphrase to encrypt the RSA key (aes-128) • background {on <DEVICE-NAME>} – Performs the operation in the background • on <DEVICE-NAME> – On an AP or a Controller • <DEVICE-NAME> – On AP/Controller name

key generate	• generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {on <DEVICE-NAME>} – Generates a keypair • rsa <WORD> – Enter the name of a RSA keypair to generate • <1024-2048> – Enter the size of the RSA key in bits from 1024-2048 • on <DEVICE-NAME> – On an AP or a Controller • <DEVICE-NAME> – On AP/Controller name
key import	• import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}|passphrase} – Performs an import operation • rsa <RSA-KEYPAIR-NAME> – Enter the name of a RSA keypair to import • <IMPORT-FROM-URL> {background|on|phrase} – Enter the location to send the key using the following formats: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • background {on <DEVICE-NAME>} – Performs the operation in the background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • passphrase <KEY-PASSPHRASE>> {background|on} – Enter a passphrase to decrypt the RSA key (aes-128) • background {on <DEVICE--NAME>} – Performs the operation in background • on <DEVICE-NAME> – On an AP or a Controller
key zeroize	• zeroize rsa <RSA-KEYPAIR-NAME> {force {on <DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-NAME>} – Performs delete operation • rsa <RSA-KEYPAIR-NAME> – Deletes the specified RSA key • force {on <DEVICE-NAME>} – Forces the deletion of all certificates associated with the key • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name
pki [authenticate|export|generate|import|zeroize]	Performs PKI related commands

pki authenticate <trustpoint-name> <URL> *{background} {on <DEVIICE-name>}*	• authenticate <TRUSTPOINT-NAME> – Authenticates and imports ca certificate • <URL> (background|on} – Enter the location of ca certificate to authenticate tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • {background} {on <DEVICE-NAME>} – Performs the operation in the background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]	• export – Performs export operation • request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name] [<EXPORT-TO-URL>|email|fqdn|ip-address] – Generates and exports a Certificate Signing Request • generate-rsa-key <RSA-KEYPAIR-NAME> – Generates a new RSA key-pair • use-rsa-key – Uses a generated RSA key-pair The following parameters are common for the above: • RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name] – Enter the name of RSA key-pair to export • autogen-subject-name – Autogenerates the subject name from config parameters • URL – Enter the URL to export the CSR tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • email – Enter the email address • fqdn – Enter the fully qualified domain name • ip-address – Enter the IP Address

	• subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> {email <EMAIL>|fqdn <FQDN>|ip-address <IP>|on <DEVICE-OR-DOMAIN-NAME> – Enter the subject name to identify the certificate • <COMMON-NAME> – Enter the common name to be used with the ca certificate • <COUNTRY> – Enter the deployment country (2 character ISO code) • <STATE> – Enter the state (2 to 64 characters) • <CITY> – Enter the city (2 to 64 characters) • <ORGANIZATION> – Enter the organization name (2 to 64 characters) • <ORGANIZATION-UNIT> – Enter the organization unit name (2 to 64 characters) • email <WORD> – Enter the email address • fqdn – Enter the fully qualified domain name • ip-address <A.B.C.D> – Enter the IP Address • on <DEVICE-NAME > – On AP/Controller • <DEVICE-NAME> – AP/Controller name
export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> *{background} {on <DEVICE-NAME>}*	Exports a trustpoint (CA cert, CRL, server cert and private key). • <TRUSTPOINT-NAME> – Enter the trustpoint name • <EXPORT-TO-URL> (background|on} – Enter the location of ca certificate to import URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • background {on <DEVICE-NAME>} – Performs the operation in background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>	• generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name] – Generates Operation • self-assigned – Generates a self-signed certificate (and trustpoint with it) • <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] – Enter the trustpoint name • generate-rsa-key – Generates a new RSA key-pair • use-rsa-key – Uses a generated RSA key-pair The following parameters are common for the above: • <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name] – Enter the name of RSA key-pair to export • autogen-subject-name – Autogenerates the subject name from config parameters • URL – Enter the URL to export the CSR to URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • email – Enter a destination email address • fqdn – Enter the fully qualified domain name • ip-address – Enter an IP Address • subject-name <Common-Name> <Country> <State> <City> <Organization> <Organization-Unit> {email<WORD>|fqdn <WORD>|ip-address <A.B.C.D>|on} <DEVICE-OR-DOMAIN-NAME> – Enter the subject name to identify the certificate • <Common-Name> – Enter the common name used with the certificate • <Country> – Enter the country (2 character ISO code) • State – Enter the state (2 to 64 characters) • City – Enter the city (2 to 64 characters) • <Organization> – Enter the Organization name (2 to 64 characters) • <Organization-Unit> {email <WORD>|fqdn <WORD>|ip-address <A.B.C.D>|on} – Enter the Organization unit name (2 to 64 characters) • email <WORD> – Enter the email address • fqdn – Enter the fully qualified domain name • ip-address <A.B.C.D> – Enter the IP Address • on <DEVICE-NAME > – On AP/Controller • <DEVICE-NAME> – AP/Controller name

import [certificate|crl|trustpoint]	Imports certificates, certificate revocation list or a trustpoint to the selected device. • certificate <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {on <DEVICE-NAME>}|on <DEVICE-NAME>} – Imports the signed server certificate • <TRUSTPOINT-NAME> – Enter the name of the trustpoint (should be already authenticated) • <IMPORT-FROM-URL> – Enter the URL to import from URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • crl <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {on<DEVICE-NAME>}|on <DEVICE-NAME>} – Imports a Certificate revocation list • <TRUSTPOINT-NAME> – Enter the name of trustpoint to which CRL belongs • <IMPORT-FROM-URL> – URL to import CRL from URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file The following parameters are common for certificate and crl: • background {on <DEVICE-NAME>} – Performs the operation in background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

	• trustpoint <WORD> URL {background {on <DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-NAME>|passphrase <word> {background {on <DEVICE--NAME>}|on <DEVICE-NAME>} – Imports a trustpoint, includes CA certificate, server certificate and private key • <WORD> – Enter the name of the trustpoint name • URL (background|on} – Enter the location to import trustpoint from URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • background {on <DEVICE-NAME>} – Performs the operation in background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller name • passphrase <WORD> {background|on} – Enter a passphrase if the private key is to be exported encrypted) • background {on <DEVICE-NAME>} – Performs the operation in background • zeroise trustpoint <TRUSTPOINT-NAME> {del-key} {on <DEVICE-NAME>} – Performs delete operation • trustpoint <WORD> – Enter the name of the trustpoint to delete • del-key {on <DEVICE-NAME>} – Deletes the private key associated to the server certificate • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE>crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs7000-37FABE>

rfs7000-37FABE>crypto key import rsa moto123 url passphrase word background on
rfs7000-37FABE
RSA key import operation is started in background
rfs7000-37FABE>

rfs7000-37FABE>crypto pki generate self-signed word generate-rsa-key word autogen-
subject-name fqdn word
Successfully generated self-signed certificate
rfs7000-37FABE>

rfs7000-37FABE#crypto pki zeroize trustpoint word del-key on rfs7000-37FABE
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using default-
trustpoint
rfs7000-37FABE#

rfs7000-37FABE>crypto pki authenticate word url background on rfs7000-37FABE
Import of CA certificate started in background
rfs7000-37FABE>

rfs7000-37FABE>crypto pki import trustpoint word url passphrase word on rfs7000-37FABE
Import operaton started in background
rfs7000-37FABE>
```

2.1.10 disable

User Exec Commands

Turns off (disables) the privileged mode command set. This command is not applicable to the User Executable mode.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
disable
```

Parameters

None

Example

```
rfs7000-37FABE>disable
rfs7000-37FABE>
```

2.1.11 enable

User Exec Commands

Turns on (enables) the privileged mode command set. This command is not applicable in the Privilege Executable mode.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
enable
```

Parameters

None

Example

```
rfs7000-37FABE>enable
rfs7000-37FABE#
```

2.1.12 exit

User Exec Commands

Ends the current CLI session and closes the session window.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE>exit ?
```

2.1.13 help

User Exec Commands

Describes the interactive help system.

Use this command to access the advanced help feature. Use "**?**" anytime at the command prompt to access the help topic.

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
help {show configuration-tree|search}
help search <WORD> {detailed|only-show|skip-show}
```

Parameters

show configuration-tree	Displays running system information • configuration-tree – Displays the relationships among configuration objects, laid out as a tree
search <WORD> {detailed|only-show|skip-show}	Searches for CLI commands related to a specific term • <WORD> – Enter a term to search CLI commands for (Eg: a feature or a configuration parameter) • detailed – Searches and displays help strings in addition to mode and commands • only-show – Displays only "show" commands, not the configuration commands • skip-show – Displays only configuration commands, not "show" commands

Example

```
rfs7000-37FABE>help search crypto detailed
Found 29 references for "crypto"

Mode    : User Exec
Command : show crypto key rsa (|public-key-detail) (|(on DEVICE-OR-DOMAIN-NAME))
           \ Show running system information
            \ Encryption related commands
             \ Key management operations
              \ Show RSA public Keys
               \ Show the public key in PEM format
                \ On AP/Controller or RF-Domain
                 \ AP / Controller / RF-Domain name

        : show crypto pki trustpoints (WORD|all|)(|(on DEVICE-OR-DOMAIN-NAME))
           \ Show running system information
            \ Encryption related commands
             \ Public Key Infrastructure related commands
              \ Display the configured trustpoints
               \ Display a particular trustpoint's details
                \ Display details for all trustpoints
                 \ On AP/Controller or RF-Domain
                  \ AP / Controller / RF-Domain name

        : show crypto isakmp sa (|(on DEVICE-NAME))
           \ Show running system information
            \ Encryption Module
             \ Show ISAKMP related statistics
              \ Show all ISAKMP Security Associations
               \ On AP/Controller
                \ AP / Controller name

        : show crypto ipsec sa (|(on DEVICE-NAME))
           \ Show running system information
            \ Encryption Module
             \ Show IPSec related statistics
              \ IPSec security association
               \ On AP/Controller
                \ AP / Controller name

        : clear crypto isakmp sa (A.B.C.D|all) (|(on DEVICE-NAME))
           \ Clear
            \ Encryption Module
             \ ISAKMP database
              \ Flush ISAKMP SAs
               \ Fluch ISAKMP SAs for a given peer
................................................................................
.....................................................................rfs7000-37FABE>

rfs7000-37FABE>help show configuration-tree

 ## ACCESS-POINT / Controller ## ---+
                                    |
                                    +--> [[ RF-DOMAIN ]]
                                    |
                                    +--> [[ PROFILE ]]
                                    |
                                 +--> Device specific parameters (license, serial number,
hostname)
                                    |
                                    +--> Configuration Overrides of rf-domain and profile

 ## RF-DOMAIN ## ---+
                    |
                    +--> RF parameters, WIPS server parameters
                    |
                    +--> [[ SMART-RF-POLICY ]]
                    |
                    +--> [[ WIPS POLICY ]]
```

```
 ## PROFILE ## ---+
                  |
                  +--> Physical interface (interface GE,ME,UP etc)
                  |                          |
                  |                          +--> [[ RATE-LIMIT-TRUST-POLICY ]]
                  |
                  +--> Vlan interface (interface VLAN1/VLAN36 etc)
                  |
                  +--> Radio interface (interface RADIO1, RADIO2 etc)
                  |                          |
                  |                          +--> Radio specific Configuration
                  |                          |
                  |                          +--> [[ RADIO-QOS-POLICY ]]
                  |                          |
                  |                          +--> [[ ASSOC-ACL-POLICY ]]
                  |                          |
                  |                          +--> [[ WLAN ]]
                  |
                  +--> [[ MANAGEMENT-POLICY ]]
                  |
                  +--> [[ DHCP-SERVER-POLICY ]]
                  |
                  +--> [[ FIREWALL-POLICY ]]
                  |
                  +--> [[ NAT-POLICY ]]
.............................................................................
.....................................................rfs7000-37FABE>

rfs7000-37FABE>help search clrscr only-show
found no commands containing "clrscr"
rfs7000-37FABE>


rfs7000-37FABE>help search service skip-show
Found 32 references for "service"

Mode    : User Exec
Command : service show cli
        : service show rim config (|include-factory)
        : service show wireless credential-cache
        : service show wireless neighbors
        : service show general stats(|(on DEVICE-OR-DOMAIN-NAME))
        : service show process(|(on DEVICE-OR-DOMAIN-NAME))
        : service show mem(|(on DEVICE-OR-DOMAIN-NAME))
        : service show top(|(on DEVICE-OR-DOMAIN-NAME))
        : service show crash-info (|(on DEVICE-OR-DOMAIN-NAME))
        : service cli-tables-skin
(none|minimal|thin|thick|stars|hashes|percent|ansi|utf-8) (grid|)
        : service cli-tables-expand (|left|right)
        : service wireless clear unauthorized aps (|(on DEVICE-OR-DOMAIN-NAME))
        : service wireless qos delete-tspec AA-BB-CC-DD-EE-FF tid <0-7>
        : service wireless wips clear-event-history
        : service wireless wips clear-mu-blacklist (all|(mac AA-BB-CC-DD-EE-FF))
        : service radio <1-3> dfs simulate-radar (primary|extension)
        : service smart-rf run-calibration
        : service smart-rf stop-calibration
        : service cluster manual-revert
        : service advanced-wips clear-event-history
        : service advanced-wips clear-event-history (dos-eap-failure-spoof|id-theft-
out-of-sequence|id-theft-eapol-success-spoof-detected|wlan-jack-attack-
detected|essid-jack-attack-detected|monkey-jack-attack-detected|null-probe-response-
detected|fata-jack-detected|fake-dhcp-server-detected|crackable-wep-iv-used|windows-
zero-config-memory-leak|multicast-all-systems-on-subnet|multicast-all-routers-on-
subnet|multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-
detection|multicast-rip2-routers-detection|multicast-igmp-routers-
detection|multicast-vrrp-agent|multicast-hsrp-agent|multicast-dhcp-server-relay-
agent|multicast-igmp-detection|netbios-detection|stp-detection|ipx-
detection|invalid-management-frame|invalid-channel-advertized|dos-deauthentication-
detection|dos-disassociation-detection|dos-rts-flood|rogue-ap-detection|accidental-
```

```
association|probe-response-flood|dos-cts-flood|dos-eapol-logoff-storm|unauthorized-
bridge)
        : service start-shell
        : service pktcap on(bridge|drop|deny|router|wireless|vpn|radio (all|<1-3>)
(|promiscuous)|rim|interface `WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>')(|{direction
(any|inbound|outbound)|acl-name WORD|verbose|hex|count <1-1000000>|snap <1-
2048>|write (FILE|URL|tzsp WORD)|tcpdump})(|filter LINE)

Mode    : Profile Mode
Command : service watchdog

Mode    : Radio Mode
Command : service antenna-type (default|dual-
band|omni|yagi|embedded|panel|patch|sector|out-omni|in-patch|ap650-int)
        : service disable-erp
        : service disable-ht-protection
        : service recalibration-interval <0-65535>
.....................................................................rfs7000-
37FABE>

rfs7000-37FABE>help search mint only-show
Found 8 references for "mint"

Mode    : User Exec
Command : show mint neighbors (|details)(|(on DEVICE-NAME))
        : show mint links (|details)(|(on DEVICE-NAME))
        : show mint id(|(on DEVICE-NAME))
        : show mint stats(|(on DEVICE-NAME))
        : show mint route(|(on DEVICE-NAME))
        : show mint lsp
        : show mint lsp-db (|details)(|(on DEVICE-NAME))
        : show mint mlcp(|(on DEVICE-NAME))
rfs7000-37FABE>
```

2.1.14 logging

User Exec Commands

Modifies message logging facilities.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
logging monitor {<0-7>|alerts|critical|debugging|
emergencies|errors|informational|notifications|warnings}
```

Parameters

monitor {<0-7>|alerts|critical|debugging| emergencies|errors| informational|notifications| warnings}	• monitor – Sets the terminal lines logging level
	  • <0-7> – Enter the logging severity level from 0-7
	  • alerts – Immediate action needed (severity=1)
	  • critical – Critical conditions (severity=2)
	  • debugging – Debugging messages (severity=7)
	  • emergencies – System is unusable (severity=0)
	  • errors – Error conditions (severity=3)
	  • informational – Informational messages (severity=6)
	  • notifications – Normal but significant conditions (severity=5)
	• warnings – Warning conditions (severity=4)

Example

```
rfs7000-37FABE>logging monitor warnings ?
 rfs7000-37FABE>

rfs7000-37FABE>logging monitor 2
rfs7000-37FABE>
```

2.1.15 mint

User Exec Commands

Configures MiNT protocol

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mint [ping|traceroute]
mint ping MINT-ID {count <1-60>|size <1-64000>|timeout <1-10>}
mint traceroute MINT-ID {destination-port <1-65535>|max-hops <1-255>|
source-port <1-65535>|timeout <1-255>}
```

Parameters

ping MINT-ID { count <1-60>| size <1-64000>| timeout <1-10>	Sends a MiNT echo message to a MiNT destination • MINT-ID – Enter the MiNT destination ID to ping • count <1-60> – Enter the number of times to ping from1-60. The default value is 3 • size <1-64000> – Enter the size of the MiNT payload in bytes from 1-64000. The default value is 64 • timeout <1-10> – Enter the time for a response after sending a ping request from 1-10 seconds. The default timeout is 1 second
traceroute MINT-ID { destination-port <1-65535>| max-hops <1-255>| source-port <1-65535>| timeout <1-255>}	Print the route packets trace to a device • MINT-ID – Enter the MiNT destination id • destination-port <1-65535> – Enter the destination port value to be used for ECMP (default 45) • max-hops <1-255> – Enter the maximum number of hops, a traceroute packet traverses in forward direction.(default 30) • source-port <1-65535> – Enter the source port value to be used for ECMP (default 45) • timeout <1-65535> – Enter the time to wait for a response (default 30 seconds)

Example

```
rfs7000-37FABE>mint ping 70.37.FA.BF count 20 size 128
MiNT ping 70.37.FA.BF with 128 bytes of data.
 Response from 70.37.FA.BF: id=1 time=0.292 ms
 Response from 70.37.FA.BF: id=2 time=0.206 ms
 Response from 70.37.FA.BF: id=3 time=0.184 ms
 Response from 70.37.FA.BF: id=4 time=0.160 ms
 Response from 70.37.FA.BF: id=5 time=0.138 ms
 Response from 70.37.FA.BF: id=6 time=0.161 ms
 Response from 70.37.FA.BF: id=7 time=0.174 ms
 Response from 70.37.FA.BF: id=8 time=0.207 ms
 Response from 70.37.FA.BF: id=9 time=0.157 ms
```

```
 Response from 70.37.FA.BF: id=10 time=0.153 ms
 Response from 70.37.FA.BF: id=11 time=0.159 ms
 Response from 70.37.FA.BF: id=12 time=0.173 ms
 Response from 70.37.FA.BF: id=13 time=0.156 ms
 Response from 70.37.FA.BF: id=14 time=0.209 ms
 Response from 70.37.FA.BF: id=15 time=0.147 ms
 Response from 70.37.FA.BF: id=16 time=0.203 ms
 Response from 70.37.FA.BF: id=17 time=0.148 ms
 Response from 70.37.FA.BF: id=18 time=0.169 ms
 Response from 70.37.FA.BF: id=19 time=0.164 ms
 Response from 70.37.FA.BF: id=20 time=0.177 ms

--- 70.37.FA.BF ping statistics ---
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 0.138/0.177/0.292 ms
```

2.1.16 no

User Exec Commands

Use the no command to revert a command or to set parameters to their default values. This command is useful if you would like to turn off an enabled feature or set default values for a parameter

NOTE: The commands have their own set of parameters that can be reset.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [adoption|captive-portal|crypto|debug|logging|page|service|
terminal|wireless]
```

Parameters

None

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE>no adoption
rfs7000-37FABE>

rfs7000-37FABE>no page
rfs7000-37FABE>

rfs7000-37FABE>no service cli-tables-expand line
rfs7000-37FABE>
```

2.1.17 page

User Exec Commands

Use the command to toggle the Controller paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
page
```

Parameters

None

Example

```
rfs7000-37FABE>page
rfs7000-37FABE>
```

2.1.18 ping

User Exec Commands

Sends ICMP echo messages to a user-specified location

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`ping {[<IP>|<hostname>]}`

Parameters

ping {[<IP>|<hostname>]}	Pings the specified destination IP address or hostname. When entered without any parameters, this command prompts for an IP/Host-name to ping.

Example

```
rfs7000-37FABE>ping 172.16.10.3
PING 172.16.10.3 (172.16.10.3): 100 data bytes
108 bytes from 172.16.10.3: seq=0 ttl=64 time=7.100 ms
108 bytes from 172.16.10.3: seq=1 ttl=64 time=0.390 ms
108 bytes from 172.16.10.3: seq=2 ttl=64 time=0.422 ms
108 bytes from 172.16.10.3: seq=3 ttl=64 time=0.400 ms

--- 172.16.10.3 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.390/2.078/7.100 ms
rfs7000-37FABE>
```

2.1.19 revert

User Exec Commands

Reverts the changes made in the active session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
revert
```

Parameters

None

Example

```
rfs7000-37FABE>revert
rfs7000-37FABE>
```

2.1.20 service

User Exec Commands

The service command performs different functions depending on the parameter passed to it. Generally, this command is used to directly interact with the device to force an action to be performed

NOTE: Service commands have their own set of parameters that can be used. Please refer to the *Chapter 5, service* for a list of parameters used with this command.

Syntax

```
service [advanced-wips|clear|cli-tables-expand|cli-tables-skin|cluster|
   force-send-config|locator|noc|radio|radius|set|show|smart-rf|wireless|pktcap]
```

Parameters

NOTE: Please see *Chapter 5, service* for more information on the parameters.

Example

```
rfs7000-37FABE>service  locator
rfs7000-37FABE>service set validation-mode full
rfs7000-37FABE>rfs7000-37FABE>service show sysinfo
System Information:

Free RAM:  65.2% (166672 of 255464)  Min: 10.0%
File Descriptors: free: 24070 used: 1088 max: 25500
CPU load averages: 1 min: 0.5%  5 min: 0.5%  15 min: 0.4%

Kernel Buffers:
Size:       32    64   128   256   512    1k    2k    4k    8k   16k   32k   64k  128k
Usage:    2592  2983   858   162   296   112   136    25    71     1     1     2     0
Limit:   32768  8192  4096  4096  8192  8192 16384 16384  1024   512   256    64    64
rfs7000-37FABE>
```

2.1.21 show

User Exec Commands

Displays the settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances
- When invoked with the display_parameter, it displays information about that component.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show <parameter>
```

Parameters

NOTE:

NOTE: Refer to '*Chapter 6, SHOW COMMANDS*' for more information.

Example

```
rfs7000-37FABE>show ?
 adoption                    Display information related to adoption to wireless
                           controller
  advanced-wips            Advanced WIPS
  captive-portal           Captive portal commands
  cdp                      Cisco Discovery Protocol
  clock                    Display system clock
  cluster                  Cluster Protocol
  commands                 Show command lists
  context                  Information about current context
  critical-resources       Critical Resources
  crypto                   Encryption related commands
  debug                    Debugging functions
  debugging                Debugging functions
  device-categorization    Device Categorization
  event-history            Display event history
  firewall                 Wireless Firewall
  interface                Interface Configuration/Statistics commands
  ip                       Internet Protocol (IP)
  licenses                 Show installed licenses and usage
  mac-address-table        Display MAC address table
  mint                     MiNT protocol
  noc                      Noc-level information
  ntp                      Network time protocol
  password-encryption      Pasword encryption
  power                    Show power over ethernet command
  remote-debug             Show details of remote debug sessions
  rf-domain-manager        Show RF Domain Manager selection details
```

```
  role                    Role based firewall
  running-config          Current operating configuration
  session-changes         Configuration changes made in this session
  session-config          This session configuration
  sessions                Display CLI sessions
  smart-rf                Smart-RF Management Commands
  spanning-tree           Display spanning tree information
  startup-config          Startup configuration
  terminal                Display terminal configuration parameters
  timezone                The timezone
  version                 Display software & hardware version
  wireless                Wireless commands
rfs7000-37FABE>
```

2.1.22 telnet

User Exec Commands

Opens a telnet session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`telnet <IP> {port}`

Parameters

<IP> {port}	Defines an IP address or hostname of a remote system • port – Enter the TCP port number

Example

```
rfs7000-37FABE>telnet 172.16.10.1

Entering character mode
Escape character is '^]'.
RFS7000 release 5.0.0.0-061D
rfs7000-37FABE login: cli
NOTE: logging in as 'cli' w/o password is going away. Use admin accounts under
management-policy [Eg: admin/motorola]
Welcome to CLI
rfs7000-37FABE>
```

2.1.23 terminal

User Exec Commands

Sets the length/number of lines displayed within the terminal window

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
terminal [length|width] <0-512>
```

Parameters

length <0-512>	Sets the number of lines on a screen
width <0-512>	Sets the width/number of characters on the screen line

Example

```
rfs7000-37FABE>terminal length 150
rfs7000-37FABE>

rfs7000-37FABE>terminal width 215
rfs7000-37FABE>
```

2.1.24 time-it

User Exec Commands

Verifies the time taken by a particular command between request and response

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
time-it <LINE>
```

Parameters

<LINE>	Verifies the time taken by a particular command between request and response • <LINE> – Specify the command to view the response

Example

```
rfs7000-37FABE>time-it enable
That took 0.00 seconds..
rfs7000-37FABE#
```

2.1.25 traceroute

User Exec Commands

Traces the route to a defined destination. Use the '--help' or '-h' built in to see a complete list of parameters for the traceroute command.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
traceroute <LINE>
```

Parameters

<LINE>	Traces the route to a destination IP address or a hostname

Example

```
rfs7000-37AFBE>traceroute --help
BusyBox v1.14.1 () multi-call binary

Usage: traceroute [-FIldnrv] [-f 1st_ttl] [-m max_ttl] [-p port#] [-q nqueries]
        [-s src_addr] [-t tos] [-w wait] [-g gateway] [-i iface]
        [-z pausemsecs] HOST [data size]

Trace the route to HOST

Options:
        -F      Set the don't fragment bit
        -I      Use ICMP ECHO instead of UDP datagrams
        -l      Display the ttl value of the returned packet
        -d      Set SO_DEBUG options to socket
        -n      Print hop addresses numerically rather than symbolically
        -r      Bypass the normal routing tables and send directly to a host
        -v      Verbose
        -m max_ttl      Max time-to-live (max number of hops)
        -p port#        Base UDP port number used in probes
                        (default is 33434)
        -q nqueries     Number of probes per 'ttl' (default 3)
        -s src_addr     IP address to use as the source address
        -t tos          Type-of-service in probe packets (default 0)
        -w wait         Time in seconds to wait for a response
                        (default 3 sec)
        -g              Loose source route gateway (8 max)
rfs7000-37FABE>traceroute 172.16.10.2
traceroute to 172.16.10.2 (172.16.10.2), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  3002.008 ms !H  3002.219 ms !H  3003.945 ms !H
rfs7000-37FABE>
```

2.1.26 watch

User Exec Commands

Repeats the specific CLI command at a periodic interval

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
watch <1-3600> <LINE>
```

Parameters

<1-3600> <LINE>	Repeats the specified CLI command in the given time intervals. Select a time frame from 1-3600 seconds

Example

```
rfs7000-37FABE>watch 45 page
rfs7000-37FABE>
```

2.1.27 write

User Exec Commands

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
write
```

Parameters

memory	Writes to the NV memory
terminal	Writes to terminal

Example

```
rfs7000-37FABE>write memory
[OK]
rfs7000-37FABE>


rfs7000-37FABE>write terminal
!
! Configuration of RFS7000 version 5.0.0.0-061D
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 enable
 calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
 voice-prioritization
 svp-prioritization
 wmm background cw-max 8
 wmm video txop-limit 9
.....................................................................
rfs7000-37FABE>
```

CHAPTER 3 PRIVILEGED EXEC MODE COMMANDS

Most PRIV EXEC commands set operating parameters. Privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes commands contained within the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the host name of the device followed by a pound sign (#).

To access the PRIV EXEC mode, enter the following at the prompt:

```
rfs7000-37FABE>enable
rfs7000-37FABE#
```

The PRIV EXEC mode is often referred to as the enable mode, because the enable command is used to enter the mode. There is no provision to configure a password to get access to PRIV EXEC (enable) mode.

NOTE: This chapter contains only those commands which are specific to Privilege Exec Mode only and not present in User Exec Mode. For all other common commands, refer to *Chapter 2, User Exec Mode Commands*.

```
rfs7000-37FABE#?
Priv Exec commands:
  ap-upgrade      AP firmware upgrade
  archive         Manage archive files
  boot            Boot commands
  cd              Change current directory
  change-passwd   Change password
  clear           Clear
  clock           Configure software system clock
  cluster         Cluster commands
  commit          Commit all changes made in this session
  configure       Enter configuration mode
  connect         Open a console connection to a remote device
  copy            Copy from one file to another
  crypto          Encryption related commands
  debug           Debugging functions
  delete          Deletes specified file from the system.
  diff            Display differences between two files
  dir             List files on a filesystem
  disable         Turn off privileged mode command
  edit            Edit a text file
  enable          Turn on privileged mode command
  erase           Erase a filesystem
  format          Format file system
  halt            Halt the system
```

```
  help            Description of the interactive help system
  logging         Modify message logging facilities
  mint            MiNT protocol
  mkdir           Create a directory
  more            Display the contents of a file
  no              Negate a command or set its defaults
  page            Toggle paging
  ping            Send ICMP echo messages
  pwd             Display current directory
  reload          Halt and perform a warm reboot
  remote-debug    Troubleshoot remote system(s)
  rename          Rename a file
  revert          Revert changes
  rmdir           Delete a directory
  self            Config context of the device currently logged into
  service         Service Commands
  show            Show running system information
  telnet          Open a telnet connection
  terminal        Set terminal line parameters
  time-it         Check how long a particular command took between request and
                  completion of response
  traceroute      Trace route to destination
  upgrade         Upgrade software image
  upgrade-abort   Abort an ongoing upgrade
  watch           Repeat the specific CLI command at a periodic interval
  write           Write running configuration to memory or terminal

  clrscr          Clears the display screen
  exit            Exit from the CLI

rfs7000-37FABE#
```

3.1 Privileged Exec Mode Commands

Table 3.1 Summarizes the PRIV EXEC commands:.

Table 3.1 *Privileged Exec Commands*

Command	Description	Reference
ap-upgrade	Upgrades firmware on access point devices	*page 3-5*
archive	Manages file archive operations	*page 3-8*
boot	Specifies the image used after reboot	*page 3-9*
cd	Changes the current directory	*page 3-10*
change-passwd	Changes the password of a logged user	*page 3-11*
clear	Clears parameters, cache entries, table entries, and other similar entries	*page 3-12*
clock	Configures the system clock	*page 3-15*
clrscr	Clears the display screen	*page 3-16*
cluster	Initiates a cluster context	*page 3-17*
commit	Commits all the changes made in the current active session	*page 3-19*
configure	Enters the configuration mode	*page 3-18*
connect	Begins a console connection to a remote device	*page 3-20*
copy	Copies a file from any location to the controller	*page 3-21*
crypto	Enables encryption	*page 3-22*
delete	Deletes a specified file from the system	*page 3-31*
diff	Displays the differences between 2 files	*page 3-33*
dir	Displays the list of files on a filesystem	*page 3-34*
edit	Edits a text file	*page 3-35*
enable	Turns on (enables) the privileged mode commands set	*page 3-36*
erase	Erases a filesystem	*page 3-37*
exit	Ends the current CLI session and closes the session window	*page 3-38*
format	Formats the file system	*page 3-39*
halt	Stops the controller	*page 3-40*
help	Describes the interactive help system	*page 3-41*
logging	Modified message logging facilities	*page 3-45*
mint	Configures MiNT protocols	*page 3-47*
mkdir	Creates a new directory in the filesystem	*page 3-46*

Table 3.1 *Privileged Exec Commands*

Command	Description	Reference
more	Displays the contents of a file	*page 3-49*
no	Reverts a command or sets values to their default settings	*page 3-50*
page	Toggles the Controller paging function.	*page 3-51*
ping	Sends ICMP echo messages to a user-specified location	*page 3-52*
pwd	Displays the current directory	*page 3-53*
reload	Halts the controller and performs a warm reboot	*page 3-54*
rename	Renames a file in the existing filesystem	*page 3-55*
revert	Reverts the changes made in the active session	*page 3-56*
rmdir	Deletes an existing file from the file system	*page 3-57*
self	Displays the configuration context of the device	*page 3-58*
service	Performs different functions depending on the parameter passed to it.	*page 3-59*
show	Displays the settings for the specified system component	*page 3-60*
telnet	Opens a telnet session	*page 3-62*
terminal	Sets the length/number of lines displayed within the terminal window	*page 3-63*
time-it	Verifies the time taken by a particular command between request and response	*page 3-64*
traceroute	Traces the route to a defined destination.	*page 3-65*
upgrade	Upgrades the software image	*page 3-66*
upgrade-abort	Aborts an ongoing software image upgrade	*page 3-67*
watch	Repeats the specific CLI command at a periodic interval	*page 3-68*
write	Writes the system running configuration to memory or terminal	*page 3-69*

3.1.1 ap-upgrade

Privileged Exec Mode Commands

Enables automatic adopted AP firmware upgrade

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap-upgrade [<DEVICE-NAME>|all|ap650|ap6511|ap6532|ap71xx|cancel-upgrade|
   load-image|rf-domain]
ap-upgrade [<DEVICE-NAME>|ap650|ap6511|ap6532|ap71xx] all {no-reboot|
   reboot-time <TIME>|upgrade-time <TIME>}]
ap-upgrade all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>}
ap-upgrade cancel-upgrade [<DEVICE-NAME>|ap650|ap6511|ap6532|ap71xx] all
ap-upgrade cancel-upgrade all
ap-upgrade cancel-upgrade on rf-domain [<RF-DOMAINNAME>|all]
ap-upgrade load-image [ap650|ap6511|ap6532|ap71xx] <URL>

ap-upgrade rf-domain <rf-domainname> [all|ap650|ap6511|ap6532|
   ap71xx] {no-reboot|no-via-rf-domain|reboot-time <TIME>|
   upgrade-time <TIME>}
ap-upgrade rf-domain all [all|ap650|ap6511|ap6532|ap71xx]
   {no-reboot|no-via-rf-domain|reboot-time <TIME>|upgrade-time <TIME>}
```

Parameters

[<DEVICE-NAME>|all|ap650 |ap71xx|ap6511|ap6532|] [cancel-upgrade|load-image| rf-domain]	• <DEVICE-NAME> all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Specify the name/MAC address of an AP • all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades all the access points • ap650 all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades an AP650 device • ap6511 all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades an AP6511 device • ap6532 all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades an AP6532 device • ap71xx all {no-reboot|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades an AP71xx device • cancel-upgrade [<DEVICE-NAME>|ap650|ap6532|ap71xx| ap6511|all] – Cancels upgrading the AP • load-image [ap650|ap71xx|ap6511] <URL> – Loads the AP firmware images on the Controller • <URL> – Specify the location of firmware image URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • rf-domain <RF-DOMAINNAME> {no-reboot|no-via-rf-domain|reboot-time <TIME>|upgrade-time <TIME>} – Upgrades all the access points belonging to an RF Domain • no-via-rf-domain – Upgrades APs from the adopted device The following are common for all the above: • no-reboot – No reboot (manually reboot after the upgrade) • reboot-time <TIME> – Sets the scheduled reboot time • upgrade-time <TIME> – Sets the scheduled upgrade time • <TIME> – Specify the reboot time in MM/DD/YYYY-HH:MM or HH:MM format

Example

```
rfs7000-37FABE>ap-upgrade ap650 00-A0-F8-00-00-00
rfs7000-37FABE>
rfs7000-37FABE>ap-upgrade all
rfs7000-37FABE>
rfs4000-880DA7>ap-upgrade  default/rfs4000-880DA7 no-reboot
-------------------------------------------------------------------------
CONTROLLER                STATUS                    MESSAGE
-------------------------------------------------------------------------
00-23-68-88-0D-A7          Success          Queued 0 APs to upgrade
-------------------------------------------------------------------------
rfs4000-880DA7>
rfs7000-37FABE#ap-upgrade rfs7000-37FABE reboot-time 06/01/2011-12:10
```

```
-------------------------------------------------------------------------
CONTROLLER              STATUS                  MESSAGE
-------------------------------------------------------------------------
00-15-70-37-FA-BE       Success          Queued 0 APs to upgrade
-------------------------------------------------------------------------
rfs7000-37FABE#
```

3.1.2 archive

Privileged Exec Mode Commands

Manages file archive operations

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
archive tar /table [<FILE>|<URL>]
archive tar /create [<FILE>|<URL>] <FILE>
archive tar /xtract [<FILE>|<URL>] <DIR>
```

Parameters

tar	Manipulates (creates, lists or extracts) a tar file
/table	Lists the files in a tar file
/create	Creates a tar file
/xtract	Extracts content from a tar file
<FILE>	Defines a Tar filename
<URL>	Sets the tar file URL
<DIR>	A directory name. When used with /create, the dir is the source directory for the tar file. When used with /xtract, the dir is the destination file where the contents of the tar file are extracted.

Example

How to zip the folder flash:/log/?

```
rfs7000-37FABE#archive tar /create flash:/out.tar flash:/log/
tar: Removing leading '/' from member names
flash/log/
flash/log/snmpd.log
flash/log/messages.log
flash/log/startup.log
flash/log/radius/
rfs7000-37FABE#dir flash:/
```

3.1.3 boot

Privileged Exec Mode Commands

Specifies the image used after reboot

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
boot system [primary|secondary] {on <DEVICE-NAME>}
```

Parameters

system [primary|secondary] {on <DEVICE-NAME>}	Specifies the image used after a device reboot
	• primary – Primary image used after reboot
	• secondary – Secondary image used after reboot
	  • on <DEVICE-NAME> – On AP/Controller
	  • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE#boot system primary on rfs7000-37FABE
Rebooting with primary partition
rfs7000-37FABE#
```

3.1.4 cd

Privileged Exec Mode Commands

Changes the current directory

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`cd {<DIR>}`

Parameters

<DIR>	Changes the current directory to DIR. This parameter is optional. When this parameter is not provided, the current directory name is displayed.

Example

```
rfs7000-37FABE#cd
nvram:/   system:/  flash:/

rfs7000-37FABE#cd flash:/?
  DIR  Change current directory to DIR

rfs7000-37FABE#cd flash:/
flash:/backup/     flash:/crashinfo/  flash:/hotspot/    flash:/log/
flash:/out/

rfs7000-37FABE#cd flash:/log/?
  DIR  Change current directory to DIR

rfs7000-37FABE#cd flash:/log/
rfs7000-37FABE#pwd
flash:/log/
rfs7000-37FABE#
```

3.1.5 change-passwd

Privileged Exec Mode Commands

Changes the password of the logged in user

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
change-passwd {<OLD-PASSWD> <NEW-PASSWD>}
```

Parameters

{<OLD-PASSWD> <NEW-PASSWD>}	Optional. The passwords can also be changed interactively. To do so, press Enter after the change-passwd command. • <OLD-PASSWD> – The password needing to be changed • <NEW-PASSWD> – The new password to update to.

Usage Guidelines

A password must be between 8 to 32 characters in length.

Example

```
rfs7000-37FABE#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
rfs7000-37FABE>write memory
OK
rfs7000-37FABE>
```

3.1.6 clear

Privileged Exec Mode Commands

Clears parameters, cache entries, table entries, and other similar entries. The clear command is only available for specific commands. The information cleared using this command varies depending on the mode where the clear command is executed.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

NOTE: Refer to the interface details below when using `clear`

- ge <index> – RFS4000 supports 4GEs and RFS6000 supports 8 GEs
- me1– Available in both RFS7000 and RFS6000

Syntax

```
clear [arp-cache|cdp|counters|crypto|event-history|firewall|ip|lldp|
   spanning-tree]
clear arp-cache {on <DEVICE-NAME>}
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
clear crypto [ipsec|isakmp] sa [<IP>|all] {on <DEVICE-NAME>}
clear event-history
clear firewall [dhcp snoop-table|dos stats|flows] {on <DEVICE-NAME>}
clear ip dhcp bindings [<A.B.C.D>|all] {on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface {<INTERFACE>|
   ge <1-8>|me1|port-channel <1-4>|vlan <1-4094>} {on <DEVICE-NAME>}

clear counters [all|bridge|router|thread]
clear counters interface [<INTERFACE>|all|ge <1-8>|me1|
   port-channel <1-4>|vlan <1-4094>]
```

Parameters

arp-cache *{on <DEVICE--NAME>}*	Clears ARP cache entries. • on <DEVICE-NAME> – Optional. Clears the arp cache on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name
[cdp|lldp] neighbors *{on <DEVICE-NAME>}*	Clears Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) neighbor table entries • neighbors – Clears CDP neighbor table • on <DEVICE-NAME> – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name
clear counters [all|bridge|router|thread] clear counters interface [<INTERFACE>|all|ge <1-8>|me1| port-channel <1-4>|vlan <1-4094>]	Clears the different counters available on the system. • all – Clears all counters • bridge – Clears the bridge counters • router – Clears the router counters • thread – Clears the thread counters • interface [<INTERFACE>|all|ge <1-8>|me1|port-channel <1-4>|vlan <1-4094>] – Clears the interface counters for the specified interface.
crypto [ipsec|isakmp] sa [<IP>|all] {on <DEVICE-NAME>}	Clears the encryption module's databases. • ipsec sa – Clears the IPSEC security associations. • isakmp sa – Clears the ISAKMP security associations. The following are common for the above: • <IP> – Clears the IPSec or ISAKMP security associations for a certain Peer. • all – Clears the IPSec or ISAKMP security associations for all Peers. • on <DEVICE-NAME> – Optional. Clears the SAs on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name
event-history	Clears event history
firewall [dhcp snoop-table|dos stats|flows] *{on <DEVICE-NAME>}*	Clears the firewall event entries. • dhcp snoop-table – Clears the DHCP Snoop Table entries • dos stats – Clears the denial of service statistics • flows – Clears the established firewall sessions. • on <DEVICE-NAME> – Optional. Clears the SAs on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name

ip dhcp bindings [<IP>|all] *{on <DEVICE-NAME>}*	Clears the DHCP address bindings. • on <DEVICE-NAME> – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name
spanning-tree detected-protocols {interface {<INTERFACE>|ge <1-8>|me1|port-channel <1-4>|vlan <1-4094>} {on <DEVICE-NAME>}	Clears the spanning-tree protocols configured for the interface • detected-protocols *{interface [<INTERFACE>|ge <1-8>|me1|port-channel <1-4>|vlan <1-4094>]} {on}* – Enter the interface name to clear the detected spanning tree protocols for that specific interface • <INTERFACE> – Clears the selected interface name • ge < 1-8> – Clears the configured GigabitEthernet interface status • me1– Clears the FastEthernet interface status • port-channel <1-4> – Clears the port-channel information on a AP/Controller • vlan <1-4094> – Clears the configured vlan information • wwan1– Clears the Wireless WAN interface information The following are common for the above • on <DEVICE-NAME> – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller • <DEVICE-NAME> – An AP or a Controller name

Example

```
rfs7000-37FABE#clear crypto isakmp sa 111.222.333.01 on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE#clear event-history
rfs7000-37FABE#

rfs7000-37FABE#clear firewall dos stats on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE#clear spanning-tree detected-protocols interface port-channel 1 on
rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE#clear ip dhcp bindings 172.16.10.9 on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE#clear cdp neighbors on rfs7000-37FABE
rfs7000-37FABE#
rfs4000-880DA7#clear spanning-tree detected-protocols interface ge 1
rfs4000-880DA7#

rfs4000-880DA7#clear lldp neighbors
rfs4000-880DA7#
```

3.1.7 clock

Privileged Exec Mode Commands

Configures the system clock

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

Parameters

set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}	• Sets the software system clock for the configured device • <HH:MM:SS> – Sets the current time (in military format hours, minutes and seconds) • <1-31> – Enter the numerical day of the month • <MONTH> – Enter the month of the year (Jan to Dec) • <1993-2035> – Select a valid digit year from 1993-2035 • on – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE#clock set 12:30:45 2 MONTH 2010 on rfs7000-37FABE
clock set 12:30:45 2 MONTH 2010 on rfs7000-37FABE rfs7000-37FABE>
```

3.1.8 clrscr

Privileged Exec Mode Commands

Clears the screen and refreshes the prompt (**#**)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clrscr
```

Parameters

None

Example

```
rfs7000-37FABE#clrscr
rfs7000-37FABE#
```

3.1.9 cluster

Privileged Exec Mode Commands

Use this command to initiate the cluster context. The cluster context provides centralized management to configure all the cluster members from any one member.

Any commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
cluster start-selection
```

Parameters

start-selection	Starts a new cluster master election

Example

```
rfs7000-37FABE#cluster start-election
rfs7000-37FABE#
```

3.1.10 configure

Privileged Exec Mode Commands

Enters the configuration mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`configure {self|terminal}`

Parameters

self	Enables configuration from the terminal
terminal	Enables the configuration mode of the current device

Example

```
rfs7000-37FABE#configure self
Enter configuration commands, one per line.  End with CNTL/Z.
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#

rfs7000-37FABE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs7000-37FABE(config)#
```

3.1.11 commit

Privileged Exec Mode Commands

Commits all the changes made in the active session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`commit {write memory}`

Parameters

write memory	If a commit succeeds, the configuration is written to memory • memory – Writes the changes to memory

Example

```
rfs7000-37FABE#commit write memory
[OK]
rfs7000-37FABE#
```

3.1.12 connect

Privileged Exec Mode Commands

Begins a console connection to a remote device using the remote device's MINT ID or its device name.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
connect [mint-id <MINT-ID>|<REMOTE-DEVICE-NAME>]
```

Parameters

mint-id <MINT-ID>	Connects to the remote system using MINT ID. • <MINT-ID> – The MINT ID of the remote device.
<REMOTE-DEVICE-NAME>	Connects to the remote system using its device name.

Example

```
rfs7000-37FABE#connect  RFDOMAIN_UseCase1/rfs7000-37FAAA

Entering character mode
Escape character is '^]'.
RFS7000 release 5.1.0.0-061D
rfs7000-37FABE login: admin
Password:
Welcome to CLI
rfs7000-37FAAA>
```

3.1.13 copy

Privileged Exec Mode Commands

Copies file (config,log,txt ...etc) from any location to the controller and vice-versa

NOTE: Copying a new config file onto an existing running-config file merges it with the existing running-config on the controller. Both the existing running-config and the new config file are applied as the current running-config.

Copying a new config file onto a start-up config files replaces the existing start-up config file with the parameters of the new file. It is better to erase the existing start-up config file and then copy the new config file to the startup config.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
copy [FILE|URL] [FILE|URL]
```

Parameters

FILE	The first <FILE> is the source file to copy from. The second <FILE> is the destination to copy.
URL	The first <URL> is the source URL to copy from. The second <URL> is the destination URL to copy.

Example

Transferring file snmpd.log to remote tftp server?

```
rfs7000-37FABE#copy flash:/log/snmpd.log
tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote tftp server into switch running-config?

```
rfs7000-37FABE#copy tftp://157.235.208.105:/running-config running-config
```

3.1.14 crypto

Privileged Exec Mode Commands

Enables encryption

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
crypto [key|pki]

crypto key [export|generate|import|zeroise]
crypto key export rsa <RSA-KEYPAIR-NAME>> <EXPORT-TO-URL>
   {background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
    {background} {on <DEVICE-NAME>}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {passphrase <KEY-
PASSPHRASE>} {background} {on <DEVICE-NAME>}

crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048>
   {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
    {background} {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> passphrase <KEY-
PASSPHRASE> {background} {on <DEVICE-NAME>}

crypto key  zeroise rsa <RSA-KEYPAIR-NAME> {force} {on <DEVICE-NAME>}

crypto pki [authenticate|export|generate|import|zeroise]
crypto pki authenticate <TRUST-POINT> <URL> {background} {on <DEVICE-NAME>}

crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|use-rsa-key]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-
subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-
subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn <FQDN>,ip-address <IP>)

crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> autogen-
subject-name <EXPORT-TO-URL> {background} {on <DEVICE-NAME>}

crypto pki export request [generate-rsa-key|use-rsa-key] <WORD> subject-name <COMMON-
NAME> <COUNTRY>  <STATE> <CITY> <ORGANISATION> <ORGANIZATION-UNIT> [<EXPORT-TO-
URL>|email <SEND-TO-EMAIL>|fqdn <FQDN>|ip-address <IP>]

crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {{background} {on
<DEVICE--NAME>}|passphrase <KEY-PHRASE> {background} {on <DEVICE-NAME>}|on <DEVICE-
NAME>}}

crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> [autogen-subject-name|subject-name]

crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name {email|fqdn|ip-address|on}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name email <WORD> {fqdn <WORD>|ip-address <A.B.C.D>|on
<DEVICE-NAME>}
crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name fqdn <WORD> {email <WORD>|ip-address <A.B.C.D>|on
<DEVICE-NAME>}
crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name ip-address <A.B.C.D> {fqdn <WORD>|on <DEVICE-NAME>}
crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> autogen-subject-name {on <DEVICE-NAME>}

crypto pki generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key]
<WORD> subject-name <COMMON-NAME> <COUNTRY>  <STATE> <CITY> <ORGANISATION>
<ORGANIZATION-UNIT> {email <WORD>|fqdn <WORD>|ip-address <A.B.C.D>|on} <DEVICE-NAME>

crypto pki import [certificate|crl|trustpoint]
crypto pki import [certificate|crl] <WORD> <IMPORT-FROM-URL> {background {on <DEVICE-
NAME>}|on <DEVICE--NAME>}]

crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background {on
<DEVICE-NAME>}|on <DEVICE-NAME>|passphrase <word> {background {on <DEVICE-NAME>}|on
<DEVICE-OR-DOMAIN-NAME>}

crypto pki zeroise trustpoint <TRUSTPOINT-NAME> {del-key {on
<DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-NAME>}
```

Parameters

key	Performs key management operations
key export	• export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {background|on|phrase} – Performs export operation • rsa <RSA-KEYPAIR-NAME> – Enter the name of a RSA keypair to export • <EXPORT-TO-URL> {background|on|phrase} – Enter the location to send the key to using the following syntax: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • background {on <DEVICE-NAME>} – Performs the operation in background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • passphrase <KEY-PASSPHRASE> {background|on} – Enter a passphrase to encrypt the RSA key (aes-128) • background {on <DEVICE-NAME>} – Performs the operation in the background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

key generate	• generate rsa <RSA-KEYPAIR-NAME> <1024-2048> {on <DEVICE-NAME>} – Generates a keypair • rsa <WORD> – Enter the name of a RSA keypair to generate • <1024-2048> – Enter the size of the RSA key in bits from 1024-2048 • on <DEVICE-NAME> – On an AP or a Controller • <DEVICE-NAME> – On AP/Controller name
key import	• import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background {on <DEVICE-NAME>}|on <DEVICE-NAME>}|passphrase} – Performs an import operation • rsa <RSA-KEYPAIR-NAME> – Enter the name of a RSA keypair to import • <IMPORT-FROM-URL> {background|on|phrase} – Enter the location to send the key using the following formats: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • background {on <DEVICE-NAME>} – Performs the operation in the background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • passphrase <KEY-PASSPHRASE>> {background|on} – Enter a passphrase to decrypt the RSA key (aes-128) • background {on <DEVICE--NAME>} – Performs the operation in background • on <DEVICE-NAME> – On an AP or a Controller
key zeroize	• zeroize rsa <RSA-KEYPAIR-NAME> {force {on <DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-NAME>} – Performs delete operation • rsa <RSA-KEYPAIR-NAME> – Deletes the specified RSA key • force {on <DEVICE-NAME>} – Forces the deletion of all certificates associated with the key • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name
pki [authenticate|export|generate|import|zeroize]	Performs PKI related commands

pki authenticate <trustpoint-name> <URL> *{background} {on <DEVIICE-name>}*	• authenticate <TRUSTPOINT-NAME> – Authenticates and imports ca certificate • <URL> (background|on} – Enter the location of ca certificate to authenticate tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • {background} {on <DEVICE-NAME>} – Performs the operation in the background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name]	• export – Performs export operation • request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name] [<EXPORT-TO-URL>|email|fqdn|ip-address] – Generates and exports a Certificate Signing Request • generate-rsa-key <RSA-KEYPAIR-NAME> – Generates a new RSA key-pair • use-rsa-key – Uses a generated RSA key-pair The following parameters are common for the above: • RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name] – Enter the name of RSA key-pair to export • autogen-subject-name – Autogenerates the subject name from config parameters • URL – Enter the URL to export the CSR tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • email – Enter the email address • fqdn – Enter the fully qualified domain name • ip-address – Enter the IP Address

	• subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> {email <EMAIL>|fqdn <FQDN>|ip-address <IP>|on <DEVICE-OR-DOMAIN-NAME> – Enter the subject name to identify the certificate • <COMMON-NAME> – Enter the common name to be used with the ca certificate • <COUNTRY> – Enter the deployment country (2 character ISO code) • <STATE> – Enter the state (2 to 64 characters) • <CITY> – Enter the city (2 to 64 characters) • <ORGANIZATION> – Enter the organization name (2 to 64 characters) • <ORGANIZATION-UNIT> – Enter the organization unit name (2 to 64 characters) • email <WORD> – Enter the email address • fqdn – Enter the fully qualified domain name • ip-address <A.B.C.D> – Enter the IP Address • on <DEVICE-NAME > – On AP/Controller • <DEVICE-NAME> – AP/Controller name
export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> *{background} {on <DEVICE-NAME>}*	Exports a trustpoint (CA cert, CRL server cert and private key). • <TRUSTPOINT-NAME> – Enter the trustpoint name • <EXPORT-TO-URL> (background|on} – Enter the location of ca certificate to import URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • background {on <DEVICE-NAME>} – Performs the operation in background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

generate self-signed <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>	• generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name] – Generates Operation • self-assigned – Generates a self-signed certificate (and trustpoint with it) • <TRUSTPOINT-NAME> [generate-rsa-key|use-rsa-key] – Enter the trustpoint name • generate-rsa-key – Generates a new RSA key-pair • use-rsa-key – Uses a generated RSA key-pair The following parameters are common for the above: • <RSA-KEYPAIR-NAME> [autogen-subject-name|subject-name] – Enter the name of RSA key-pair to export • autogen-subject-name – Autogenerates the subject name from config parameters • URL – Enter the URL to export the CSR to URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • email – Enter a destination email address • fqdn – Enter the fully qualified domain name • ip-address – Enter an IP Address • subject-name <Common-Name> <Country> <State> <City> <Organization> <Organization-Unit> {email<WORD>|fqdn <WORD>|ip-address <A.B.C.D>|on} <DEVICE-OR-DOMAIN-NAME> – Enter the subject name to identify the certificate • <Common-Name> – Enter the common name used with the certificate • <Country> – Enter the country (2 character ISO code) • State – Enter the state (2 to 64 characters) • City – Enter the city (2 to 64 characters) • <Organization> – Enter the Organization name (2 to 64 characters) • <Organization-Unit> {email <WORD>|fqdn <WORD>|ip-address <A.B.C.D>|on} – Enter the Organization unit name (2 to 64 characters) • email <WORD> – Enter the email address • fqdn – Enter the fully qualified domain name • ip-address <A.B.C.D> – Enter the IP Address • on <DEVICE-NAME > – On AP/Controller • <DEVICE-NAME> – AP/Controller name

import [certificate|crl|trustpoint]	Imports certificates, certificate revocation list or a trustpoint to the selected device. • certificate <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {on <DEVICE-NAME>}|on <DEVICE-NAME>} – Imports the signed server certificate • <TRUSTPOINT-NAME> – Enter the name of the trustpoint (should be already authenticated) • <IMPORT-FROM-URL> – Enter the URL to import from URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • crl <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background} {on <DEVICE-NAME>}|on <DEVICE-NAME>} – Imports a Certificate revocation list • <TRUSTPOINT-NAME> – Enter the name of trustpoint to which CRL belongs • <IMPORT-FROM-URL> – URL to import CRL from URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file The following parameters are common for certificate and crl: • background {on <DEVICE-NAME>} – Performs the operation in background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

	• trustpoint <WORD> URL {background {on <DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-NAME>|passphrase <word> {background {on <DEVICE--NAME>}|on <DEVICE-NAME>} – Imports a trustpoint, includes CA certificate, server certificate and private key • <WORD> – Enter the name of the trustpoint name • URL (background|on} – Enter the location to import trustpoint from URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file http://<hostname|IP>[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file • background {on <DEVICE-NAME>} – Performs the operation in the background • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • on <DEVICE-NAME>} – On AP/Controller • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller name • passphrase <WORD> {background|on} – Enter a passphrase if the private key is to be exported encrypted) • background {on <DEVICE-NAME>} – Performs the operation in the background • zeroise trustpoint <TRUSTPOINT-NAME> {del-key} {on <DEVICE-NAME>} – Performs delete operation • trustpoint <WORD> – Enter the name of the trustpoint to delete • del-key {on <DEVICE-NAME>} – Deletes the private key associated to the server certificate • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE>crypto key generate rsa key 1025
RSA Keypair successfully generated
rfs7000-37FABE>

rfs7000-37FABE>crypto key import rsa moto123 url passphrase word background on
rfs7000-37FABE
RSA key import operation is started in background
rfs7000-37FABE>

rfs7000-37FABE>crypto pki generate self-signed word generate-rsa-key word autogen-
subject-name fqdn word
Successfully generated self-signed certificate
rfs7000-37FABE>

rfs7000-37FABE#crypto pki zeroize trustpoint word del-key on rfs7000-37FABE
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using default-
trustpoint
rfs7000-37FABE#

rfs7000-37FABE>crypto pki authenticate word url background on rfs7000-37FABE
Import of CA certificate started in background
rfs7000-37FABE>

rfs7000-37FABE>crypto pki import trustpoint word url passphrase word on rfs7000-37FABE
Import operaton started in background
rfs7000-37FABE>
```

3.1.15 delete

Privileged Exec Mode Commands

Deletes a specified file from the system

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

Parameters

/force	Forces deletion without a prompt
/recursive	Performs a recursive delete
<FILE>	Specifies the filename(s) to delete

Example

```
rfs7000-37FABE#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

rfs7000-37FABE#delete /force flash:/tmp.txt
rfs7000-37FABE#

rfs7000-37FABE#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk

[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz

[y/n]? n
rfs7000-37FABE#
```

3.1.16 disable

Privileged Exec Commands

Turns off (disables) the privileged mode command set. This command is not applicable to the User Executable mode.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
disable
```

Parameters

None

Example

```
rfs7000-37FABE>disable
rfs7000-37FABE>
```

3.1.17 diff

Privileged Exec Mode Commands

Displays the differences between 2 files

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

Parameters

FILE	The first <FILE> is the source file for the diff. The second <FILE> is the file to compare.
URL	The first <URL> is the source URL for the diff. The second <URL> is the url to compare.

Example

```
rfs7000-37FABE#diff startup-config running-config
--- startup-config
+++ running-config
@@ -1,3 +1,4 @@
+!### show running-config
 !
 ! Configuration of RFS7000 version 5.1.0.0-061D
 !
@@ -80,7 +81,6 @@
  excluded-address 172.16.10.9 172.16.10.10
  bootp ignore
 !
-gui default
 !
 firewall-policy default
 !
rfs7000-37FABE#
```

3.1.18 dir

Privileged Exec Mode Commands

Use this command to view the list of files on a filesystem

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`dir {[/all|/recursive|<DIR>|all-filesystems]}`

Parameters

/all	Lists all files
/recursive	Lists files recursively
<DIR>	Lists files in the named file path
all-filesystems	Lists the files on all filesystems

Example

```
rfs7000-37FABE# dir
Directory of flash:/.

  drwx             Thu Apr 29 12:36:29 2010   log
  -rw-   39        Tue Dec 29 11:41:00 2009   FILE
  drwx             Thu Apr 29 11:34:11 2010   crashinfo
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Mon Dec 14 14:09:39 2009   TestDir
  drwx             Fri Dec 11 15:38:25 2009   Testdir

rfs7000-37FABE#
rfs7000-37FABE#dir all-filesystems
Directory of flash:/

  drwx             Thu Apr 29 12:36:29 2010   log
  -rw-   39        Tue Dec 29 11:41:00 2009   FILE
  drwx             Thu Apr 29 11:34:11 2010   crashinfo
  drwx             Sat Jan  1 00:00:25 2000   hotspot
  drwx             Mon Dec 14 14:09:39 2009   TestDir
  drwx             Fri Dec 11 15:38:25 2009   Testdir

Directory of nvram:/

  -rw-   3460      Fri Dec 11 14:42:44 2009   startup-config.save
  -rw-   1638      Tue Jan  5 14:27:17 2010   startup-config-unused
  -rw-   3393      Mon Dec 14 13:55:51 2009   startup-config.save.1
  -rw-   8059      Thu Apr 29 12:36:27 2010   startup-config

Directory of system:/

  drwx             Thu Apr 29 12:35:52 2010   proc

rfs7000-37FABE#
```

3.1.19 edit

Privileged Exec Mode Commands

Edits a text file

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
edit <FILE>
```

Parameters

<FILE>	Name of the file to be modified

Example

```
rfs7000-37FABE#edit startup-config
  GNU nano 1.2.4                                        File: startup-config

!
! Configuration of RFS7000 version 5.1.0.0-061D
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 enable
 calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
 voice-prioritization
 svp-prioritization
 wmm background cw-max 8
 wmm video txop-limit 9
 wmm voice cw-min 6
 wmm voice cw-max 6
 rate-limit client to-air max-burst-size 3
 rate-limit client to-air red-threshold video 101
 rate-limit client from-air rate 55
 rate-limit client from-air red-threshold background 100
 rate-limit client from-air red-threshold voice 1010
!
!
```

3.1.20 enable

Privileged Exec Mode Commands

Turns on (enables) the privileged mode command set. This command is not applicable in the Privilege Executable mode.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
enable
```

Parameters

None

Example

```
rfs7000-37FABE>enable
rfs7000-37FABE#
```

3.1.21 erase

Privileged Exec Mode Commands

Erases a filesystem

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
erase [cf:|flash:|nvram:|startup-config|usb1]
```

Parameters

cf:	Erases everything in controller cf:
flash:	Erases everything in controller flash:
nvram:	Erases everything in controller nvram:
startup-config	Erases everything in controller usb2:
usb1:	Erases everything in controller usb1:

Example

```
rfs7000-37FABE#erase startup-config
Erase startup-config? (y/n): n
rfs7000-37FABE#
```

3.1.22 exit

Privileged Exec Mode Commands

Ends the current CLI session and closes the session window.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE#exit ?
```

3.1.23 format

Privileged Exec Mode Commands

Formats file system

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
format cf:
```

Parameters

cf:	Formats compact flash

Example

```
rfs7000-37FABE#format cf:
Warning: This will destroy the contents of compact flash.
Do you want to continue [y/n]? n
rfs7000-37FABE#
```

3.1.24 halt

Privileged Exec Mode Commands

Stops (halts) the Controller

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`halt {on <DEVICE-NAME>}`

Parameters

{on <DEVICE-NAME>}	• on – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE#halt on rfs7000-37FABE
rfs7000-37FABE#
```

3.1.25 help

Privileged Exec Mode Commands

Describes the interactive help system.

Use this command to access the advanced help feature. Use "**?**" anytime at the command prompt to access the help topic.

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
help {show configuration-tree|search}
help search <WORD> {detailed|only-show|skip-show}
```

Parameters

show configuration-tree	Displays running system information • configuration-tree – Displays the relationships among configuration objects, laid out as a tree
search <WORD> {detailed|only-show|skip-show}	Looks for CLI commands related to a specific term • <WORD> – Enter a term to search CLI commands for (Eg: a feature or a configuration parameter) • detailed – Searches and displays help strings in addition to mode and commands • only-show – Displays only "show" commands, not the configuration commands • skip-show – Displays only configuration commands, not "show" commands

Example

```
rfs7000-37FABE#help search crypto detailed
Found 29 references for "crypto"

Mode    : Priv Exec
Command : show crypto key rsa (|public-key-detail) (|(on DEVICE-OR-DOMAIN-NAME))
           \ Show running system information
            \ Encryption related commands
             \ Key management operations
              \ Show RSA public Keys
               \ Show the public key in PEM format
                \ On AP/Controller or RF-Domain
                 \ AP / Controller / RF-Domain name

        : show crypto pki trustpoints (WORD|all|)(|(on DEVICE-OR-DOMAIN-NAME))
           \ Show running system information
            \ Encryption related commands
             \ Public Key Infrastructure related commands
              \ Display the configured trustpoints
               \ Display a particular trustpoint's details
                \ Display details for all trustpoints
                 \ On AP/Controller or RF-Domain
                  \ AP / Controller / RF-Domain name

        : show crypto isakmp sa (|(on DEVICE-NAME))
           \ Show running system information
            \ Encryption Module
             \ Show ISAKMP related statistics
              \ Show all ISAKMP Security Associations
               \ On AP/Controller
                \ AP / Controller name

        : show crypto ipsec sa (|(on DEVICE-NAME))
           \ Show running system information
            \ Encryption Module
             \ Show IPSec related statistics
              \ IPSec security association
               \ On AP/Controller
                \ AP / Controller name

        : clear crypto isakmp sa (A.B.C.D|all) (|(on DEVICE-NAME))
           \ Clear
            \ Encryption Module
             \ ISAKMP database
              \ Flush ISAKMP SAs
               \ Fluch ISAKMP SAs for a given peer
................................................................................
.....................................................................rfs7000-37FABE>

rfs7000-37FABE#help show configuration-tree

 ## ACCESS-POINT / Controller ## ---+
                                   |
                                   +--> [[ RF-DOMAIN ]]
                                   |
                                   +--> [[ PROFILE ]]
                                   |
                                +--> Device specific parameters (license, serial number,
hostname)
                                   |
                                   +--> Configuration Overrides of rf-domain and profile

 ## RF-DOMAIN ## ---+
                    |
                    +--> RF parameters, WIPS server parameters
                    |
                    +--> [[ SMART-RF-POLICY ]]
                    |
                    +--> [[ WIPS POLICY ]]
```

```
 ## PROFILE ## ---+
                  |
                  +--> Physical interface (interface GE,ME,UP etc)
                  |                         |
                  |                         +--> [[ RATE-LIMIT-TRUST-POLICY ]]
                  |
                  +--> Vlan interface (interface VLAN1/VLAN36 etc)
                  |
                  +--> Radio interface (interface RADIO1, RADIO2 etc)
                  |                           |
                  |                           +--> Radio specific Configuration
                  |                           |
                  |                           +--> [[ RADIO-QOS-POLICY ]]
                  |                           |
                  |                           +--> [[ ASSOC-ACL-POLICY ]]
                  |                           |
                  |                           +--> [[ WLAN ]]
                  |
                  +--> [[ MANAGEMENT-POLICY ]]
                  |
                  +--> [[ DHCP-SERVER-POLICY ]]
                  |
                  +--> [[ FIREWALL-POLICY ]]
                  |
                  +--> [[ NAT-POLICY ]]
.............................................................................
.............................................................rfs7000-37FABE>

rfs7000-37FABE#help search service skip-show
Found 32 references for "service"

Mode    : Priv Exec
Command : service show cli
        : service show rim config (|include-factory)
        : service show wireless credential-cache
        : service show wireless neighbors
        : service show general stats(|(on DEVICE-OR-DOMAIN-NAME))
        : service show process(|(on DEVICE-OR-DOMAIN-NAME))
        : service show mem(|(on DEVICE-OR-DOMAIN-NAME))
        : service show top(|(on DEVICE-OR-DOMAIN-NAME))
        : service show crash-info (|(on DEVICE-OR-DOMAIN-NAME))
        : service cli-tables-skin
(none|minimal|thin|thick|stars|hashes|percent|ansi|utf-8) (grid|)
        : service cli-tables-expand (|left|right)
        : service wireless clear unauthorized aps (|(on DEVICE-OR-DOMAIN-NAME))
        : service wireless qos delete-tspec AA-BB-CC-DD-EE-FF tid <0-7>
        : service wireless wips clear-event-history
        : service wireless wips clear-mu-blacklist (all|(mac AA-BB-CC-DD-EE-FF))
        : service radio <1-3> dfs simulate-radar (primary|extension)
        : service smart-rf run-calibration
        : service smart-rf stop-calibration
        : service cluster manual-revert
        : service advanced-wips clear-event-history
        : service advanced-wips clear-event-history (dos-eap-failure-spoof|id-theft-
out-of-sequence|id-theft-eapol-success-spoof-detected|wlan-jack-attack-
detected|essid-jack-attack-detected|monkey-jack-attack-detected|null-probe-response-
detected|fata-jack-detected|fake-dhcp-server-detected|crackable-wep-iv-used|windows-
zero-config-memory-leak|multicast-all-systems-on-subnet|multicast-all-routers-on-
subnet|multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-
detection|multicast-rip2-routers-detection|multicast-igmp-routers-
detection|multicast-vrrp-agent|multicast-hsrp-agent|multicast-dhcp-server-relay-
agent|multicast-igmp-detection|netbios-detection|stp-detection|ipx-
detection|invalid-management-frame|invalid-channel-advertized|dos-deauthentication-
detection|dos-disassociation-detection|dos-rts-flood|rogue-ap-detection|accidental-
association|probe-response-flood|dos-cts-flood|dos-eapol-logoff-storm|unauthorized-
bridge)
        : service start-shell
        : service pktcap on(bridge|drop|deny|router|wireless|vpn|radio (all|<1-3>)
(|promiscuous)|rim|interface `WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>')(|{direction
```

```
(any|inbound|outbound)|acl-name WORD|verbose|hex|count <1-1000000>|snap <1-
2048>|write (FILE|URL|tzsp WORD)|tcpdump})(|filter LINE)

Mode    : Profile Mode
Command : service watchdog

Mode    : Radio Mode
Command : service antenna-type (default|dual-
band|omni|yagi|embedded|panel|patch|sector|out-omni|in-patch|ap650-int)
        : service disable-erp
        : service disable-ht-protection
        : service recalibration-interval <0-65535>
.....................................................................rfs7000-
37FABE>

rfs7000-37FABE>help search mint only-show
Found 8 references for "mint"

Mode    : User Exec
Command : show mint neighbors (|details)(|(on DEVICE-NAME))
        : show mint links (|details)(|(on DEVICE-NAME))
        : show mint id(|(on DEVICE-NAME))
        : show mint stats(|(on DEVICE-NAME))
        : show mint route(|(on DEVICE-NAME))
        : show mint lsp
        : show mint lsp-db (|details)(|(on DEVICE-NAME))
        : show mint mlcp(|(on DEVICE-NAME))
rfs7000-37FABE>
```

3.1.26 logging

Privileged Exec Mode Commands

Modifies message logging facilities.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
logging monitor {<0-7>|alerts|critical|debugging|
emergencies|errors|informational|notifications|warnings}
```

Parameters

monitor {<0-7>|alerts|critical|debugging| emergencies|errors| informational|notifications| warnings}	• monitor – Sets the terminal lines logging level • <0-7> – Enter the logging severity level from 0-7 • alerts – Immediate action needed (severity=1) • critical – Critical conditions (severity=2) • debugging – Debugging messages (severity=7) • emergencies – System is unusable (severity=0) • errors – Error conditions (severity=3) • informational – Informational messages (severity=6) • notifications – Normal but significant conditions (severity=5) • warnings – Warning conditions (severity=4)

Example

```
rfs7000-37FABE>logging monitor warnings ?
 rfs7000-37FABE>

rfs7000-37FABE>logging monitor 2
rfs7000-37FABE>
```

3.1.27 mkdir

Privileged Exec Mode Commands

Creates a new directory in the filesystem

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mkdir <DIR>
```

Parameters

<DIR>	Directory name

Example

```
rfs7000-37FABE#mkdir testdir
rfs7000-37FABE#
```

3.1.28 mint

Privileged Exec Mode Commands

Configures MiNT protocol

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mint [ping|traceroute]
mint ping MINT-ID {count <1-60>|size <1-64000>|timeout <1-10>}
mint traceroute MINT-ID {destination-port <1-65535>|max-hops <1-255>|
source-port <1-65535>|timeout <1-255>}
```

Parameters

ping MINT-ID { count <1-60>| size <1-64000>| timeout <1-10>	Sends a MiNT echo message to a MiNT destination • MINT-ID – Enter the MiNT destination ID to ping • count <1-60> – Enter the number of times to ping from1-60. The default value is 3 • size <1-64000> – Enter the size of the MiNT payload in bytes from 1-64000. The default value is 64 • timeout <1-10> – Enter the time for a response after sending a ping request from 1-10 seconds. The default timeout is 1 second
traceroute MINT-ID { destination-port <1-65535>| max-hops <1-255>| source-port <1-65535>| timeout <1-255>}	Print the route packets trace to a device • MINT-ID – Enter the MiNT destination id • destination-port <1-65535> – Enter the destination port value to be used for ECMP (default 45) • max-hops <1-255> – Enter the maximum number of hops, a traceroute packet traverses in forward direction.(default 30) • source-port <1-65535> – Enter the source port value to be used for ECMP (default 45) • timeout <1-65535> – Enter the time to wait for a response (default 30 seconds)

Example

```
rfs7000-37FABE>mint ping 70.37.FA.BF count 20 size 128
MiNT ping 70.37.FA.BF with 128 bytes of data.
 Response from 70.37.FA.BF: id=1 time=0.292 ms
 Response from 70.37.FA.BF: id=2 time=0.206 ms
 Response from 70.37.FA.BF: id=3 time=0.184 ms
 Response from 70.37.FA.BF: id=4 time=0.160 ms
 Response from 70.37.FA.BF: id=5 time=0.138 ms
 Response from 70.37.FA.BF: id=6 time=0.161 ms
 Response from 70.37.FA.BF: id=7 time=0.174 ms
 Response from 70.37.FA.BF: id=8 time=0.207 ms
 Response from 70.37.FA.BF: id=9 time=0.157 ms
```

```
 Response from 70.37.FA.BF: id=10 time=0.153 ms
 Response from 70.37.FA.BF: id=11 time=0.159 ms
 Response from 70.37.FA.BF: id=12 time=0.173 ms
 Response from 70.37.FA.BF: id=13 time=0.156 ms
 Response from 70.37.FA.BF: id=14 time=0.209 ms
 Response from 70.37.FA.BF: id=15 time=0.147 ms
 Response from 70.37.FA.BF: id=16 time=0.203 ms
 Response from 70.37.FA.BF: id=17 time=0.148 ms
 Response from 70.37.FA.BF: id=18 time=0.169 ms
 Response from 70.37.FA.BF: id=19 time=0.164 ms
 Response from 70.37.FA.BF: id=20 time=0.177 ms

--- 70.37.FA.BF ping statistics ---
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 0.138/0.177/0.292 ms
```

3.1.29 more

Privileged Exec Mode Commands

Displays the contents of a file

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
more  <FILE>
```

Parameters

<FILE>	Displays the contents of the file

Example

```
rfs7000-37FABE#more flash:/log/messages.log
May 03 11:45:05 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/dpd2"
May 03 11:45:14 2010: %KERN-6-INFO: 0| ioctl.c:335 dev_dataplane_fw_ioctl DHCP trust
of port 0 (ge1) set to 1 by 1021 cfgd.
May 03 11:45:14 2010: %KERN-6-INFO: 0| ioctl.c:335 dev_dataplane_fw_ioctl DHCP trust
of port 1 (ge2) set to 1 by 1021 cfgd.
May 03 11:45:14 2010: %KERN-6-INFO: 0| ioctl.c:335 dev_dataplane_fw_ioctl DHCP trust
of port 2 (ge3) set to 1 by 1021 cfgd.
May 03 11:45:14 2010: %KERN-6-INFO: 0| ioctl.c:335 dev_dataplane_fw_ioctl DHCP trust
of port 3 (ge4) set to 1 by 1021 cfgd.
May 03 11:45:14 2010: %NSM-4-IFDOWN: Interface vlan1 is down
May 03 11:45:14 2010: %NSM-4-IFUP: Interface vlan4 is up
May 03 11:45:15 2010: %NSM-4-IFUP: Interface vlan44 is up
May 03 11:45:15 2010: %NSM-4-IFDOWN: Interface vlan44 is down
May 03 11:45:15 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/lighttpd"
May 03 11:45:15 2010: %FILEMGMT-5-HTTPSTART: lighttpd started in external mode with
pid 0
May 03 11:45:15 2010: %USER-5-NOTICE: FILEMGMT[1064]: FTP: ftp server stopped
May 03 11:45:15 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/telnetd"
May 03 11:45:17 2010: %AUTH-6-INFO: sshd[1371]: Server listening on 0.0.0.0 port 22.
May 03 11:45:17 2010: %AUTOINSTD-5-AUTOCLCONFDISAB: Autoinstall of cluster
configuration is disabled
May 03 11:45:17 2010: %AUTOINSTD-5-AUTOCONFDISAB: Autoinstall of startup configuration
is disabled
May 03 11:45:17 2010: %AUTOINSTD-5-AUTOIMAGEDISAB: Autoinstall of image upgrade is
disabled
May 03 11:45:18 2010: %KERN-6-INFO: dataplane enabled.
rfs7000-37FABE#
```

3.1.30 no

Privileged Exec Mode Commands

Use the no command to revert a command or to set parameters to their default values. This command is useful if you would like to turn off an enabled feature or set default values for a parameter

NOTE: The commands have their own set of parameters that can be reset.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [adoption|captive-portal|crypto|debug|logging|page|service|terminal|upgrade|
   wireless]
```

Parameters

None

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE>no adoption
rfs7000-37FABE>

rfs7000-37FABE>no page
rfs7000-37FABE>

rfs7000-37FABE>no service cli-tables-expand line
rfs7000-37FABE>
```

3.1.31 page

Privileged Exec Mode Commands

Use the command to toggle the Controller paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
page
```

Parameters

None

Example

```
rfs7000-37FABE#page
rfs7000-37FABE#
```

3.1.32 ping

Privileged Exec Mode Commands

Sends ICMP echo messages to a user-specified location

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`ping {[<IP>|<hostname>]}`

Parameters

ping {[<IP>|<hostname>]}	Pings the specified destination IP address or hostname. When entered without any parameters, this command prompts for an IP/Host-name to ping.

Example

```
rfs7000-37FABE#ping 172.16.10.3
PING 172.16.10.3 (172.16.10.3): 100 data bytes
108 bytes from 172.16.10.3: seq=0 ttl=64 time=7.100 ms
108 bytes from 172.16.10.3: seq=1 ttl=64 time=0.390 ms
108 bytes from 172.16.10.3: seq=2 ttl=64 time=0.422 ms
108 bytes from 172.16.10.3: seq=3 ttl=64 time=0.400 ms

--- 172.16.10.3 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.390/2.078/7.100 ms
rfs7000-37FABE#
```

3.1.33 pwd

Privileged Exec Mode Commands

View the contents of the current directory

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
pwd
```

Parameters

None

Example

```
rfs7000-37FABE#pwd
flash:/
rfs7000-37FABE#
```

3.1.34 reload

Privileged Exec Mode Commands

Halts the Controller and performs a warm reboot

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
reload {force {on|<DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

{force {on|<DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-OR-DOMAIN-NAME>}	• force {on|<DEVICE-OR-DOMAIN-NAME>} – Forces reboot ignoring conditions like upgrade in progress, unsaved changes etc
	  • on – On AP/Controller or RF-Domain
	  • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/ RF-Domain name
	• on <DEVICE-OR-DOMAIN-NAME>} – On AP/Controller or RF-Domain
	  • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/ RF-Domain name

Example

```
rfs7000-37FABE#reload force on rfs7000-37FABE
rfs7000-37FABE#
```

3.1.35 rename

Privileged Exec Mode Commands

Renames a file in the existing filesystem

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rename <FILE> <FILE>
```

Parameters

<FILE> <FILE>	Specifies the file to rename. The first <FILE> is the old file name. The second <FILE> defines the new file name.

Example

```
rfs7000-37FABE#rename flash:/testdir/ testdir1
rfs7000-37FABE#
```

3.1.36 revert

Privileged Exec Mode Commands

Reverts the changes made in the active session to their last saved configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
revert
```

Parameters

None

Example

```
rfs7000-37FABE#revert
rfs7000-37FABE#
```

3.1.37 rmdir

Privileged Exec Mode Commands

Deletes an existing file from the filesystem

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rmdir <DIR>
```

Parameters

<DIR>	Defines the name of the directory to delete

Example

```
rfs7000-37FABE#rmdir flash:/testdir1
rfs7000-37FABE#
```

3.1.38 self

Privileged Exec Mode Commands

Displays the configuration context of the currently logged device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
self
```

Parameters

None

Example

```
rfs7000-37FABE#self
Enter configuration commands, one per line.  End with CNTL/Z.
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

3.1.39 service

Privileged Exec Mode Commands

The service command performs different functions depending on the parameter passed to it. Generally, this command is used to directly interact with the device to force an action on the device.

NOTE: Service commands have their own set of parameters. Please refer to the *Chapter 5, service* for a list of parameters used with the service command.

Syntax

```
service [advanced-wips|clear|cli-tables-expand|cli-tables-skin|cluster|copy|force-
send-config|locator|mint|noc|pktcap|pm|radio|radius|set|show|smart-rf|start-
shell|wireless|signal
```

Parameters

NOTE: Please see *Chapter 5, service* for more information.

Example

```
rfs7000-37FABE#service start-shell
Last password used: tddxjoht with MAC 00:15:70:37:fa:be
Password:

rfs7000-37FABE#service wireless client beacon-request 11-22-33-44-55-66 mode act
ive ssid test channel-report none
```

3.1.40 show

Privileged Exec Mode Commands

Displays the settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances
- When invoked with the display_parameter, it displays information about that component.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show <parameter>
```

Parameters

NOTE:

NOTE: Refer to '*Chapter 6, show commands*' for more information.

Example

```
rfs7000-37FABE#show ?
  adoption                Display information related to adoption to wireless
                          controller
  advanced-wips           Advanced WIPS
  ap-upgrade              AP Upgrade
  boot                    Display boot configuration.
  captive-portal          Captive portal commands
  cdp                     Cisco Discovery Protocol
  clock                   Display system clock
  cluster                 Cluster Protocol
  commands                Show command lists
  context                 Information about current context
  critical-resources      Critical Resources
  crypto                  Encryption related commands
  debug                   Debugging functions
  debugging               Debugging functions
  device-categorization   Device Categorization
  event-history           Display event history
  event-system-policy     Display event system policy
  file                    Display filesystem information
  firewall                Wireless Firewall
  interface               Interface Configuration/Statistics commands
  ip                      Internet Protocol (IP)
  ip-access-list-stats    IP Access list stats
  licenses                Show installed licenses and usage
  lldp                    Link Layer Discovery Protocol
  logging                 Show logging information
  mac-access-list-stats   MAC Access list stats
```

```
mac-address-table       Display MAC address table
mint                    MiNT protocol
noc                     Noc-level information
ntp                     Network time protocol
password-encryption     Pasword encryption
power                   Show power over ethernet command
remote-debug            Show details of remote debug sessions
rf-domain-manager       Show RF Domain Manager selection details
role                    Role based firewall
running-config          Current operating configuration
session-changes         Configuration changes made in this session
session-config          This session configuration
sessions                Display CLI sessions
smart-rf                Smart-RF Management Commands
spanning-tree           Display spanning tree information
startup-config          Startup configuration
terminal                Display terminal configuration parameters
timezone                The timezone
upgrade-status          Display last image upgrade status
version                 Display software & hardware version
wireless                Wireless commands
wwan                    Display wireless WAN Status
```

3.1.41 telnet

Privileged Exec Mode Commands

Opens a telnet session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`telnet <IP> {port}`

Parameters

<IP> {port}	Defines an IP address or hostname of a remote system • port – Enter the TCP port number

Example

```
rfs7000-37FABE#telnet 172.16.10.1

Entering character mode
Escape character is '^]'.
RFS7000 release 5.1.0.0-061D
rfs7000-37FABE login: cli
NOTE: logging in as 'cli' w/o password is going away. Use admin accounts under
management-policy [Eg: admin/motorola]
Welcome to CLI
rfs7000-37FABE>
```

3.1.42 terminal

Privileged Exec Mode Commands

Sets the length/number of lines displayed within the terminal window

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
terminal [length|width] <0-512>
```

Parameters

length <0-512>	Sets the number of lines on a screen
width <0-512>	Sets the width/number of characters on the screen line

Example

```
rfs7000-37FABE#terminal length 150
rfs7000-37FABE#

rfs7000-37FABE#terminal width 215
rfs7000-37FABE#
```

3.1.43 time-it

Privileged Exec Commands

Verifies the time taken by a particular command between request and response

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
time-it <LINE>
```

Parameters

<LINE>	Verifies the time taken by a particular command between request and response • <LINE> – Specify the command to view the response

Example

```
rfs7000-37FABE#time-it enable
That took 0.00 seconds..
rfs7000-37FABE#
```

3.1.44 traceroute

Privileged Exec Mode Commands

Traces the route to a defined destination.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
traceroute <LINE>
```

Parameters

<LINE>	Traces the route to a destination IP address or hostname

Example

```
rfs7000-37FABE#traceroute 172.16.10.2
traceroute to 172.16.10.2 (172.16.10.2), 30 hops max, 38 byte packets
 1  172.16.10.1 (172.16.10.1)  3002.008 ms !H  3002.219 ms !H  3003.945 ms !H
rfs7000-37FABE>
```

3.1.45 upgrade

Privileged Exec Mode Commands

Upgrades the software image

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
upgrade <URL> {background|on <DEVICE-NAME>}
```

Parameters

<URL>	Sets the location of the target firmware image used in the upgrade
background	Optional. Specifies the upgrade should occur in the background
on <DEVICE-NAME>	on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE#upgrade tftp://157.235.208.105:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

rfs7000-37FABE#upgrade tftp://157.125.208.235/img
Running from partition /dev/mtdblock7, partition to update is /dev/mtdblock6
```

3.1.46 upgrade-abort

Privileged Exec Mode Commands

Aborts an ongoing software image upgrade

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`upgrade-abort {<on> <DEVICE-OR-DOMAIN-NAME>}`

Parameters

on <DEVICE-OR-DOMAIN-NAME>	on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF Domain • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller name/RF Domain name

Example

```
rfs7000-37FABE#upgrade-abort on rfs7000-37FABE
Error: No upgrade in progress
rfs7000-37FABE#
```

3.1.47 watch

Privileged Exec Mode Commands

Repeats the specific CLI command at a periodic interval

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
watch <1-3600> <LINE>
```

Parameters

<1-3600> <LINE>	Repeats the specified CLI command on the specified interval(s). Select an interval from 1-3600 seconds

Example

```
rfs7000-37FABE#watch 45 page
rfs7000-37FABE#
```

3.1.48 write

Privileged Exec Mode Commands

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
write
```

Parameters

memory	Writes to NV memory
terminal	Writes to terminal

Example

```
rfs7000-37FABE#write memory
[OK]
rfs7000-37FABE#


rfs7000-37FABE#write terminal
!
! Configuration of RFS7000 version 5.1.0.0-061D
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 enable
 calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
 voice-prioritization
 svp-prioritization
 wmm background cw-max 8
 wmm video txop-limit 9
rfs7000-37FABE>
```

CHAPTER 4 GLOBAL CONFIGURATION COMMANDS

This chapter summarizes the global-configuration commands in the CLI command structure.

The term global is used to indicate characteristics or features effecting the system as a whole. Use the Global Configuration Mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the configure terminal command (under PRIV EXEC) to enter the global configuration mode.

The example below describes the process of entering the global configuration mode from the privileged EXEC mode:

```
rfs7000-37FABE# configure terminal
rfs7000-37FABE(config)#
```

NOTE: The system prompt changes to indicate you are now in the global configuration mode. The prompt consists of the device host name followed by (config) and a pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a *copy running-config startup-config* EXEC command is issued.

4.1 Global Configuration Commands

Table 4.1 Summarizes global configuration commands

Table 4.1 *Global Config Commands*

Command	Description	Reference
aaa-policy	Configures an aaa-policy	*page 4-4*
advanced-wips-policy	Configures an advanced-wips-policy	*page 4-5*
ap650	Adds an AP650 access point to the controller managed network	*page 4-6*
ap6511	Adds an AP6511 access point to the controller managed network	*page 4-7*
ap6532	Adds an AP6532 access point to the controller managed network	*page 4-8*
ap71xx	Adds an AP7131 access point to the controller managed network	*page 4-9*
association-acl-policy	Configures an association-acl-policy	*page 4-10*
auto-provisioning-policy	Configures an auto provisioning policy	*page 4-11*
captive portal	Configures a captive portal	*page 4-13*
clear	Clears the event history	*page 4-29*
critical-resource-policy	Configures critical-resource-policy settings	*page 4-30*
customize	Customizes the output of summary cli commands	*page 4-35*
device	Specifies configuration on multiple devices	*page 4-40*
device-categorization	Configures a device categorization object	*page 4-41*
dhcp-server-policy	Configures a dhcp-server-policy	*page 4-46*
dns-whitelist	Configures a whitelist	*page 4-48*
do	Runs commands from the EXEC mode	*page 4-52*
event-system-policy	Configures an event system policy	*page 4-55*
firewall-policy	Configures a firewall-policy	*page 4-69*
help	Displays interactive help system	*page 4-70*
host	Sets the system's network name	*page 4-72*
igmp-snoop-policy	Configures an igmp-snoop-policy	*page 4-73*
ip	Configures a selected *Internet Protocol* (IP) component	*page 4-74*
mac	Configures MAC access lists (goes to the MAC ACL mode)	*page 4-75*
management-policy	Configures a management-policy	*page 4-76*
mint-policy	Configures a mint-security-policy	*page 4-77*
nac-list	Configures a network access control list (ACL)	*page 4-79*

Table 4.1 *Global Config Commands*

Command	Description	Reference
no	Negates a command or sets its default values	*page 4-84*
password-encryption	Enables password encryption in configuration	*page 4-86*
profile	Configures profile related commands	*page 4-87*
radio-qos-policy	Configures a radio-qos-policy	*page 4-89*
radius-group	Configures a radius-group	*page 4-90*
radius-server-policy	Configures a radius-server-policy	*page 4-91*
radius-user-pool-policy	Configures a radius-user-pool-policy	*page 4-92*
rf-domain	Creates a RF Domain	*page 4-94*
rfs4000	Adds a RFS4000 controller to the network	*page 4-99*
rfs6000	Adds a RFS6000 controller to the network	*page 4-100*
rfs7000	Adds a RFS7000 controller to the network	*page 4-101*
role-policy	Configures a role-policy	*page 4-102*
self	Displays the configuration context of the logged device	*page 4-103*
service	Retrieves system data	*page 4-104*
show	Displays running system information	*page 4-106*
smart-rf-policy	Configures a Smart-RF-policy	*page 4-108*
wips-policy	Configures a wips-policy	*page 4-109*
wlan	Configures a wireless WLAN	*page 4-111*
wlan-qos-policy	Configures a WLAN-QoS-policy	*page 4-153*
write	Writes running configuration to memory or terminal	*page 4-154*

4.1.1 aaa-policy

Global Configuration Commands

Configures an authentication/accounting/authorization policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
aaa-policy <aaa-policy-name>
```

Parameters

<aaa-policy-name>	Defines the name of the aaa-policy to be configured (will be created if it does not exist)

Example

```
rfs7000-37FABE(config)#aaa-policy test
rfs7000-37FABE(config-aaa-policy-test)#
```

NOTE: For more information, see Chapter 8, AAA-POLICY.

4.1.2 advanced-wips-policy

Global Configuration Commands

Configures an advanced-wips-policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
advanced-wips-policy <advanced-wips-policy-name>
```

Parameters

<advanced-wips-policy-name>	Sets the name of the advanced-wips policy (will be created if it does not already exist)

Example

```
rfs7000-37FABE(config)#advanced-wips-policy test
rfs7000-37FABE(config)#
```

NOTE: For more information, see Chapter 10, ADVANCED-WIPS-POLICY.

4.1.3 ap650

Global Configuration Commands

Adds an AP650 access point to the controller managed network using its MAC address. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap650 <MAC>
```

Parameters

<MAC>	Enter the MAC address of the target AP650

Example

```
rfs7000-37FABE(config)#ap650 11-22-33-44-55-66 ?
rfs7000-37FABE(config-device-11-22-33-44-55-66)

rfs7000-37FABE(config)#show wireless ap configured
+-----+-----------------+--------------------+------------------+--------
| IDX |       NAME      |         MAC        |     PROFILE      |  RF-DOMAIN  |
+-----+-----------------+--------------------+------------------+--------
| 1   | ap7131-889EC4   | 00-15-70-88-9E-C4  | default-ap7131   | default     |
| 2   | ap650-445566    | 11-22-33-44-55-66  | default-ap650    | default     |
+-----+-----------------+--------------------+------------------+--------
rfs7000-37FABE(config)#
```

4.1.4 ap6511

Global Configuration Commands

Adds an AP6511 access point to the controller network using its MAC address. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap6511 <MAC>
```

Parameters

<MAC>	Enter the MAC address of the target AP6511

Example

```
rfs7000-37FABE(config)#ap6511 00-17-70-88-9E-C4 ?
rfs7000-37FABE(config-device-00-17-70-88-9E-C4)#
```

4.1.5 ap6532

Global Configuration Commands

Adds an AP6532 access point to the controller network using its MAC address. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap6532 <MAC>
```

Parameters

<MAC>	Enter the MAC address of the target AP6532

Example

```
rfs7000-37FABE(config)#ap6532 00-27-70-89-9F-E4 ?
rfs7000-37FABE(config-device-00-27-70-89-9F-E4)#
```

4.1.6 ap71xx

Global Configuration Commands

Adds an AP71xx series access point to the controller network using its MAC address. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap71xx <MAC>
```

Parameters

<MAC>	Enter the MAC address of the target AP71xx

Example

```
rfs7000-37FABE(config)#ap71xx 00-15-70-88-9E-C4 ?
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#
```

4.1.7 association-acl-policy

Global Configuration Commands

Configures an association-acl-policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
association-acl-policy <association-acl-policy-name>
```

Parameters

<association-acl-policy-name>	Enter the name of the association-acl-policy (will be created if it does not already exist)

Example

```
rfs7000-37FABE(config)#association-acl-policy  test
rfs7000-37FABE(config)#
```

NOTE: For more information, see Chapter 11, ASSOCIATION-ACL-POLICY.

4.1.8 auto-provisioning-policy

Global Configuration Commands

Configures an auto-provisioning policy

Supported in the following platforms:

- RFs7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
auto-provisioning-policy <AUTO-PROVISIONING-POLICY>
```

Parameters

<AUTO-PROVISIONING-POLICY>	Name of the auto-provisioning policy to be configured

Example

```
rfs7000-37FABE(config)#auto-provisioning-policy test
rfs7000-37FABE(config-auto-provisioning-policy-test)#
```

NOTE: For more information see Chapter 9, AUTO-PROVISIONING-POLICY

4.1.9 captive portal

Global Configuration Commands

The Captive Portal Mode provides the commands to configure a hotspot. Table 4.2 lists the command to enter the Captive Portal configuration mode.

Table 4.2 *Captive-Portal Commands*

Command	Description	Reference
captive-portal	Configures captive portal Web page parameters	*page 4-13*

4.1.9.1 captive-portal

captive portal

Configures a captive portal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
captive-portal <CAPTIVE-PORTAL>
```

Parameters

<CAPTIVE-PORTAL>	Enter the name of the captive portal being configured (will be created if it does not exist)

Example

```
rfs7000-37FABE(config)#captive-portal testportal ?
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#captive-portal testportal
rfs7000-37FABE(config-captive-portal-testportal)#
```

4.1.9.2 captive-portal-mode commands

Table 4.3 Summarizes captive-portal mode commands

Table 4.3 *Captive-Portal-Mode Commands*

Command	Description	Reference
access-time	Defines allowed access time for a client. It's used when no session time is defined in RADIUS response	*page 4-15*
access-type	Configures the access type for a captive portal from the list	*page 4-16*
accounting	Enables accounting records for a captive portal	*page 4-17*
connection-mode	Configures the connection mode for a captive portal	*page 4-18*
custom-auth	Configures custom user information	*page 4-19*
inactivity-timeout	Defines an inactivity timeout in seconds	*page 4-20*
server	Configures the captive portal server's configuration	*page 4-21*
simultaneous-users	Specifies a particular user name that can only be used by a certain pool of MAC addresses at a time	*page 4-22*
terms-agreement	Enforces the user to agree to terms and conditions (included in login page) for captive portal access	*page 4-23*
use	Defines captive portal configuration settings	*page 4-24*
webpage-location	Specifies the location of the Web pages used for captive portal authentication	*page 4-25*
webpage	Configures captive portal Web page parameters	*page 4-26*

NOTE: The commands clrscr, commit, do, exit, help, no, revert, service, show, and write are common commands. For more information, see Chapter 5, COMMON COMMANDS.

4.1.9.2.1 access-time

critical-resource-policy

Defines the permitted access time for a client. It is used when no session time is defined in RADIUS response.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
access-time <30-10080>
```

Parameters

<30-10080>	Enter the time from <30-10080> minutes to define the allowed access time for a client.

Example

```
rfs7000-37FABE(config-captive-portal-test)#access-time 35
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.2 access-type

captive-portal-mode commands

Defines the captive portal access type

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
access-type [custom-auth-radius|logging|no-auth|radius]
```

Parameters

[custom-auth-radius| logging|no-auth|radius]	• custom-auth-radius – Verifies custom user information for authentication (RADIUS lookup with given information. For example:- Name, E-mail Address, Telephone) • logging – Generates a logging record of user access and allowed access • no-auth – No authentication for a guest is required (redirected to welcome message) • radius – Configures radius authentication

Example

```
rfs7000-37FABE(config-captive-portal-test)#access-type radius
rfs7000-37FABE(config-captive-portal-test)#

rfs7000-37FABE(config-captive-portal-testportal)#access-type logging
rfs7000-37FABE(config-captive-portal-testportal)#
```

4.1.9.2.3 accounting

captive-portal-mode commands

Enables accounting records for a captive portal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
accounting [radius|syslog]
accounting syslog host <WORD> {port} <1-65535>
```

Parameters

radius	Enables support for RADIUS accounting messages
syslog host <WORD> {port} <1-65535>	Enables support for syslog accounting messages • host <WORD> – Specify a syslog destination hostname or IP address for accounting records • {port} <1-65535> – Specify a UDP port number of syslog server between 1 and 65535

Example

```
rfs7000-37FABE(config-captive-portal-test)#accounting syslog host 172.16.10.13 port 1
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.4 connection-mode

captive-portal-mode commands

Configures the captive portal connection mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
connection-mode [http|https]
```

Parameters

[http|https]	• http – Connection-mode is http • https – Connection-mode is https

Example

```
rfs7000-37FABE(config-captive-portal-test)#connection-mode https
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.5 custom-auth

captive-portal-mode commands

Configures custom user information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
custom-auth info <LINE>
```

Parameters

info <LINE>	Information used for RADIUS lookup when custom-auth-radius access type is configured. • <LINE> – Guest data needs to be provided. Enter the name, email address and telephone number of the user

Example

```
rfs7000-37FABE(config-captive-portal-test)#custom-auth info testuser
robert@symbol.com
rfs7000-37FABE(config-captive-portal-test)#

rfs7000-37FABE(config-captive-portal-testportal)#custom-auth info bob,
bob@symbol.com, 9902833119
rfs7000-37FABE(config-captive-portal-testportal)#show context
captive-portal testportal
 access-type logging
 custom-auth info bob,\ bob@symbol.com,\ 9902833119
rfs7000-37FABE(config-captive-portal-testportal)#
```

4.1.9.2.6 inactivity-timeout

captive-portal-mode commands

Defines an inactivity timeout in seconds. If a frame is not received from a client for the specified time interval, then the current session is terminated

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
inactivity-timeout <300-1800>
```

Parameters

<300-1800>	Sets a time from 300-1800 seconds to define an inactivity timeout

Example

```
rfs7000-37FABE(config-captive-portal-test)#inactivity-timeout 750
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.7 server

captive-portal-mode commands

Configures captive portal server parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
server [host <WORD>|mode]
server mode [centralized|centralized-controller|self]
```

Parameters

[host <WORD> |mode]	• host <WORD> – Configures the address of the captive portal server
	  • <WORD> – Enter the IP address or hostname of the internal captive portal server
	• mode [centralized|centralized-controller|self] – Configures the captive portal server mode
	  • centralized – Considers the configured server hostname or IP address as the centralized captive portal server
	  • centralized-controller – Uses the configured hostname as the virtual captive portal server name across Controllers
	  • self – Selects the captive portal server as the same device supporting the WLAN

Example

```
rfs7000-37FABE(config-captive-portal-test)#server mode self
rfs7000-37FABE(config-captive-portal-test)#

rfs7000-37FABE(config-captive-portal-test)#server host 172.16.10.9
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.8 simultaneous-users

captive-portal-mode commands

Specifies a particular user name that can only be used by a certain number of MAC addresses at a time

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
simultaneous-users <0-8192>
```

Parameters

<0-8192>	Sets the number of MAC addresses allowed to use that username at the same time. Select a number between 0 and 8192 (0 implies unlimited).

Example

```
rfs7000-37FABE(config-captive-portal-test)#simultaneous-users 5
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.9 terms-agreement

captive-portal-mode commands

Enforces the user to agree to terms and conditions (included in login page) for captive portal guest access to the Controller

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
terms-agreement
```

Parameters

None

Example

```
rfs7000-37FABE(config-captive-portal-test)#terms-agreement
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.10use

captive-portal-mode commands

Defines configuration settings for the captive portal configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
use [aaa-policy <aaa-policy-name>|dns-whitelist <dns-whitelist>]
```

Parameters

[aaa-policy <aaa-policy-name>| dns-whitelist <dns-whitelist-policy>]	• aaa-policy <aaa-policy-name> – Configures a aaa-policy for the captive portal
	  • <aaa-policy-name> – Enter a policy name for authenticating captive portal users
	• dns-whitelist <dns-whitelist-policy> – Configures a DNS whitelist for the captive portal
	  • <dns-whitelist> – Enter a DNS whitelist to configure

Example

```
rfs7000-37FABE(config-captive-portal-test)#use aaa-policy test
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.11 webpage-location

captive-portal-mode commands

Specifies the location of the Web pages used for authentication. These pages can either be hosted on the system or on an external Web server

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
webpage-location [advanced|external|internal]
```

Parameters

[advanced|external|internal]	• advanced – Uses login/welcome/failure Web pages created by the user on the system • external – Uses login/welcome/failure Web pages on an external server (External URL required) • internal – Uses login/welcome/failure Web pages created automatically on the system

Example

```
rfs7000-37FABE(config-captive-portal-test)#webpage-location internal
rfs7000-37FABE(config-captive-portal-test)#

rfs7000-37FABE(config-captive-portal-test)#webpage internal agreement  title  test123
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.9.2.12webpage

captive-portal-mode commands

Configures captive portal Web page parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
webpage [external|internal]
webpage external [fail|login|welcome] <URL>
webpage internal [agreement|fail|login|welcome]
webpage internal [agreement|fail|login|welcome] [description|footer|header|main-
logo|small-logo|title]
webpage internal [agreement|fail|login|welcome] [description|footer|header|title]
<LINE>
webpage internal [agreement|fail|login|welcome] [main-logo|small-logo] <WORD>
```

Parameters

external [fail|login|welcome] <URL>]	Configures captive portal external page links • fail <URL> – Users are redirected to this Web page if they fail authentication • login <URL> – Users are prompted for their username and password on this Web page • welcome <URL> – Users are redirected to this Web page after they authenticate successfully The following parameter is common for the above: • <URL> – Enter the URL used for remote captive portal staging. The length can be to 1024 characters
internal [agreement|fail|login|welcome] [description|footer|header|main-logo|small-logo|title]	Configures captive portal internal page parameters • agreement – Users are prompted to agree the terms in this page when terms-agreement is enabled • fail – Users are redirected to this Web page if they fail authentication • login – Users are prompted for their username and password on this Web page • welcome – Users are redirected to this Web page after they authenticate successfully The following parameters are common for the above: • description <LINE> – Text displayed as the main body (normal font, middle of page) of the Web page • footer <LINE> – Text displayed at the footer (smaller font, bottom section) of the Web page • header <LINE> – Text displayed as a header (large font, top section) of the Web page • title <LINE> – Text that will be the title of the Web page The following parameter is common for the above: • <LINE> – Enter a string value. The length can be to 1024 characters • main-logo <WORD> – Main image (large size) displayed by the local Web page. Appears between the header and description on the Web-page • small-logo <WORD> – Small image (thumbnail size) displayed by the local Web page. Appears near the footer on the Web page The following parameter is common for the above: • <WORD> – Enter the URL from where the image is loaded and cached to the system

Example

```
rfs7000-37FABE(config-captive-portal-test)#webpage external fail www.symbol.com
rfs7000-37FABE(config-captive-portal-test)#
```

4.1.10 clear

Global Configuration Commands

Clears parameters, cache entries, table entries, and other similar entries. The clear command is only available for specific commands. The information cleared using this command varies depending on the mode where the clear command is executed.

In this mode, the clear command is used to clear the event history.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clear event-history
```

Parameters

event-history	Clears the event history

Example

```
rfs7000-37FABE(config)#clear event-history
rfs7000-37FABE(config)#
```

4.1.11 critical-resource-policy

Global Configuration Commands

Creates a critical resource monitoring policy. A critical resource is a device (controller, router, gateway, etc.) that is considered critical to the health of the controller managed network. This is a list of IP addresses that are pinged regularly by the wireless controller. If there is a connectivity issue with a device on the critical resource list, an event is generated stating a critical resource is unavailable. The controller does not attempt to restore connection to a critical resource. All critical devices are listed in a critical resource policy.

Table 4.4 *Critical Resource Policy Commands*

Command	Description	Reference
critical-resource-policy	Configures captive portal Web page parameters	*page 4-31*

4.1.11.1 critical-resource-policy

critical-resource-policy

Creates or enters a critical-resource policy. If the defined policy is not present, it is created.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
critical-resource-policy <CRM-Policy>
```

Parameters

<CRM-Policy>	Enter a name for the critical resource monitoring policy

Example

```
rfs7000-37FABE(config)#critical-resource-policy test
rfs7000-37FABE(config-critical-resource-policy-test)#?
 commands:
  monitor  Critical resource monitoring
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal
```

4.1.11.2 critical-resource-policy-mode

Table 4.5 Summarizes critical resource monitoring policy commands

Table 4.5 *critical-resource-policy*

Command	Description	Reference
monitor	Performs critical resource monitoring	*page 4-33*
no	Negates a command or sets its default values	*page 4-34*

4.1.11.2.1monitor

critical-resource-policy-mode

Performs critical resource monitoring

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
monitor [<IP>|ping-interval <5-86400>]
monitor <IP> ping-mode [arp-icmp|arp-only vlan <1-4094>]
```

Parameters

<IP> ping-mode [arp-icmp|arp-only vlan <1-4094>]	Enter the IP address of the critical resource to be monitored • ping-mode – Enter the protocol used for pinging a critical resource • arp-icmp – Uses either ARP requests or ICMP echo request to monitor a critical resource (requires the AP/Controller to have an IP address) • arp-only – Uses only probing arp requests to monitor a critical resource (suitable for AP/controller without IP address) • vlan <1-4094> – Enter the VLAN on which the probing ARP request has to be sent
ping-interval <5-86400>	Enter the ping interval from 5-86400 seconds

Example

```
rfs7000-37FABE(config-critical-resource-policy-test)#monitor ping-interval 10
rfs7000-37FABE(config-critical-resource-policy-test)#

rfs7000-37FABE(config-critical-resource-policy-test)#monitor 172.16.10.2 ping-mode
arp-only vlan 1
rfs7000-37FABE(config-critical-resource-policy-test)#
```

4.1.11.2.2no

critical-resource-policy-mode

Negates a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no monitor
```

Parameters

monitor	Does not monitor the specified critical resource

Example

```
rfs7000-37FABE(config-critical-resource-policy-test)#no monitor 172.16.10.2
rfs7000-37FABE(config-critical-resource-policy-test)#
```

4.1.12 customize

Global Configuration Commands

Customizes the output of summary CLI commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
customize [show-wireless-client|show-wireless-client-stats|
show-wireless-client-stats-rf|show-wireless-radio|
show-wireless-radio-stats|show-wireless-radio-stats-rf]

customize show-wireless-client [ap-name|auth|bss|enc|hostname|ip|last-
active|location|
mac|radio-alias|radio-id|radio-type|role|role-policy|state|
username|vendor|vlan|wlan]

customize show-wirless-client-stats [hostname|mac|rx-bytes|
rx-errors|
rx-packets|rx-throughput|tx-bytes|tx-dropped|tx-packets|tx-throughput]

customize show-wireless-client-stats-rf [average-retry-number|
error-rate|hostname|mac|noise|q-index|rx-rate|signal|snr|t-index|tx-rate]

customize show-wireless-radio [adopt-to|ap-name|channel|location|
num-clients|power|radio-alias|radio-id|radio-mac|rf-mode|state]

customize show-wireless-radio-stats [radio-alias|radio-id|radio-mac|
rx-bytes|rx-errors|rx-packets|rx-throughput|tx-bytes|tx-dropped|
tx-packets|tx-throughput

customize show-wireless-radio-stats-rf [average-retry-number|error-rate|noise|q-
index|radio-alias|radio-id|radio-mac|
rx-rate|signal|snr|t-index|tx-rate]
```

Parameters

show-wireless-client [ap-name|auth|bss|enc|hostname|ip|last-active| location|mac|| radio-alias|radio-id|radio-type|role|role-policy|state| username|vendor|vlan| wlan	Customizes the output of (show wireless client) commands • ap-name – Hostname of the AP to which this client associates • auth – The authentication protocol used by the client • bss – The BSSID to which the client's radio is associated to • enc – The encryption suite of the client • hostname – Hostname of the client – Configured by packet sniffing or manually • ip – The IP address of the client • last-active – Displays the last activity seen on the client • location – Location of the AP to which this client is associated to • mac – The MAC address of client • radio-alias – Consists of an AP's hostname and the radio interface number in the form of hostname:RX • radio-id – Consists of AP MAC address and the client interface number in the form of AA-BB-CC-DD-EE-FF:RX • radio-type – Radio type of the client • role – The current role of the client • role-policy – The role policy used by the client • state – The current state of the client • username – The username of the client • vendor – The vendor ID of the client • vlan – The VLAN ID assigned to the client • wlan – WLAN name
show-wireless-client-stats [hostname|mac|rx-bytes| rx-errors| rx-packets|rx-throughput| tx-bytes|tx-dropped| tx-packets|tx-throughput]	Customizes the output of (show wireless client stats) commands • hostname – The hostname of the client – Configured by sniffing packets or manually • mac – The MAC address of the client • rx-bytes – Displays the number of bytes received • rx-errors – Displays the number of errors received • rx-packets – Displays the number of packets received • rx-throughput – Displays the number of packets received per port and the percentage of port utilization • tx-bytes – Displays the number of bytes transmitted • tx-dropped – Displays the number of packets dropped during transmission • tx-packets – Displays the total number of packets transmitted • tx-throughput – Displays the number of packets transmitted per port and the percentage of port utilization

show-wireless-client-stats-rf [average-retry-number|error-rate|hostname|mac|noise|q-index|rx-rate|signal|snr|t-index|tx-rate]	Customizes the output of (show wireless client stats rf) commands • average-retry-number – Displays the average retry number per packet • error-rate – Displays the error rate • hostname – Displays the hostname of the client – Configured by sniffing packets or manually • mac – The MAC address of client • noise – Displays the noise level measured in dBm • q-index – Q-Index • rx-rate – Displays the rate of radio packets received • signal – Displays the signal strength in dBm • snr – Displays the Signal to Noise Ratio (SNR) in db • t-index – T-index • tx-rate – Displays the rate at which radio packets are transmitted
show-wireless-radio [adopt-to|ap-name|channel|location|num-clients|power|radio-alias|radio-id|radio-mac|rf-mode|state]	Customizes the output of (show wireless radio) commands • adopt-to – Displays the name of the Controller to which the client radio is adopted • ap-name – Hostname of the AP to which this radio belongs • channel – The configured and current channel of the radio • location – Location of the AP to which this radio belongs • num-clients – Number of clients associated with this radio • power – The configured and current transmit power of the radio • radio-alias – Consists of the AP's hostname and the radio interface number in the form of hostname:RX • radio-id – Consists of the AP MAC address and the radio interface number in the form of AA-BB-CC-DD-EE-FF:RX • radio-mac – The base MAC address of the radio • rf-mode – The RF mode of the radio (2.4GHz-Wlan/5GHz-wlan/sensor) • state – The current operational state of the radio

show-wireless-radio-stats [radio-alias|radio-id| radio-mac|rx-bytes|rx-errors| rx-packets|rx-throughput| tx-bytes|tx-dropped| tx-packets|tx-throughput	Customizes the output of (show wireless radio stats) commands • radio-alias – Radio alias with AP's hostname and the radio interface number in the form of hostname:RX • radio-id – Consists of the AP MAC address and the radio interface number in the form of AA-BB-CC-DD-EE-FF:RX • radio-mac – The base MAC address of the radio • rx-bytes – Displays the number of bytes received • rx-errors – Displays the number of errors receive • rx-packets – Displays the number of packets received • rx-throughput – Displays the number of packets received per port and the percentage of port utilization • tx-bytes – Displays the number of bytes transmitted • tx-dropped – Displays the number of packets dropped during transmission • tx-packets –Displays the total number of packets transmitted • tx-throughput – Displays the number of packets transmitted per port and the percentage of port utilization
show-wireless-radio-stats-rf [average-retry-number|error-rate|noise|q-index|radio-alias|radio-id|radio-mac|rx-rate|signal|snr|t-index|tx-rate]	Customizes the output of (show wireless radio stats rf) commands • average-retry-number – Displays the average retry number per packet • error-rate – Displays the error rate • noise – Displays the noise level in dBm • q-index – Q-Index • radio-alias –Consists of the AP's hostname and the radio interface number in the form of hostname:RX • radio-id – Radio ID with the AP MAC address and the radio interface number in the form of AA-BB-CC-DD-EE-FF:RX • radio-mac – The base MAC address of the radio • rx-rate – Displays the rate of radio packets received • signal – Displays the signal strength in dBm • snr – Displays the Signal to Noise Ratio in db • t-index – T-index • tx-rate – Displays the rate at which radio packets are transmitted

Example

```
rfs7000-37FABE(config)#customize show-wireless-client ap-name auth
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#customize show-wireless-client-stats mac
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#customize show-wireless-client-stats-rf average-retry-number
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#customize show-wireless-radio adopt-to
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#customize show-wireless-radio-stats radio-mac
rfs7000-37FABE(config)#
```

4.1.13 device

Global Configuration Commands

Specifies configuration on multiple devices

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
device {containing|filter}
device containing <HOSTNAME> {filter type [ap650|ap6511|ap6532|
ap71xx|rfs4000|rfs6000|rfs7000]}
device filter type [ap650|ap6511|ap6532|ap71xx|rfs4000|
rfs6000|rfs7000]
```

Parameters

{containing|filter}	• containing <HOSTNAME> filter type [ap650|ap6511|ap6532|ap71xx|rfs4000|rfs6000|rfs7000] – Optional. Specifies the devices that contain a sub-string in the host-name • filter type – Specify the additional selection filter by device type from the list of devices The following parameters are common for both containing and filter: • ap650 – AP650 access point profile • ap6511 – AP6511 access point profile • ap6532 – AP6532 access point profile • ap71xx – AP71xx access point profile • rfs4000 – RFS4000 wireless controller profile • rfs6000 – RFS6000 wireless controller profile • rfs7000 – RFS7000 wireless controller profile

Example

```
rfs7000-37FABE(config)#device containing ap filter type ap7131
% Error: Parsing cmd line (1)
rfs7000-37FABE(config)#
```

4.1.14 device-categorization

Global Configuration Commands

Categorizes devices based on different parameters.

Table 4.6 *Critical Resource Policy Commands*

Command	Description	Reference
device-categorization	Configures the device categorization lists.	page 4-42

4.1.14.1 device-categorization

Global Configuration Commands

Configures a device categorization object

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
device-categorization <device-categorization-name>
```

Parameters

<device-categorization-name>	Defines the name of device categorization list configured

Example

```
rfs7000-37FABE(config)#device-categorization rfs7000
rfs7000-37FABE(config)#

rfs7000-37FABE(config-device-categorization-rfs7000)#?
Device Category Mode commands:
  mark-device  Add a device
  no           Negate a command or set its defaults

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal
```

4.1.14.2 device-categorization-mode commands

Table 4.7 Summarizes device-categorization mode commands

Table 4.7 *device-categorization-mode commands*

Command	*Description*	*Reference*
mark-device	Adds a device to the device categorization list	*page 4-44*
no	Negates a command or sets its default values	*page 4-45*

4.1.14.2.1 mark-device

device-categorization-mode commands

Adds a device to the device categorization list

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mark-device [sanctioned|neighboring]
mark-device [sanctioned|neighboring] [ap|client]
mark-device [sanctioned|neighboring] ap [<MAC>|any] ssid [<WORD>|any]
mark-device [sanctioned|neighboring] client [<MAC>|any]
```

Parameters

[sanctioned| neighboring] [ap [<MAC> |any]|station [<MAC> |any]	• sanctioned – Marks an authorized device
	• neighboring – Marks a neighboring device
	The following parameters are common for the above:
	• ap [<MAC> |any] – Enter the MAC of an AP
	  • <MAC> ssid [<WORD>|any] – Enter an AP MAC address
	  • any ssid [<WORD>|any] – Enter any AP MAC address
	  • ssid [<WORD>|any] – Enter a particular SSID value or any SSID
	• client [<MAC> |any] – Enter a client MAC address
	  • <MAC> – Enter a particular client MAC address
	  • any – Any station (client) MAC address

Example

```
rfs7000-37FABE(config-device-categorization-rfs7000)#mark-device sanctioned ap any
ssid any
rfs7000-37FABE(config-device-categorization-rfs7000)#


rfs7000-37FABE(config-device-categorization-rfs7000)#mark-device neighboring client
11-22-33-44-55-66
rfs7000-37FABE(config-device-categorization-rfs7000)#
```

4.1.14.2.2no

device-categorization-mode commands

Removes a device from the network

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no mark-device
```

Parameters

mark-device	Removes a device

Example

```
rfs7000-37FABE(config-device-categorization-rfs7000)#no mark-device authorized ap any
ssid 1
%% Error: Parsing cmd line
rfs7000-37FABE(config-device-categorization-rfs7000)#
```

NOTE: The commands clrscr, commit, do, exit, help, write, revert, service and show are common commands. For more information, see Chapter 5, COMMON COMMANDS.

4.1.15 dhcp-server-policy

Global Configuration Commands

Configures a DHCP Server policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dhcp-server-policy <dhcp-policy -name>
```

Parameters

<dhcp-policy-name>	Enter a DHCP server policy name to configure

Example

```
rfs7000-37FABE(config)#dhcp-policy test
rfs7000-37FABE(config)#?
```

NOTE: For more information, see Chapter 13, DHCP-SERVER-POLICY.

4.1.16 dns-whitelist

Global Configuration Commands

Configures a whitelist of devices permitted to access the controller managed network or a hotspot configured for the controller managed network.

Table 4.8 *Critical Resource Policy Commands*

Command	Description	Reference
dns-whitelist	Configures the DNS whitelist.	*page 4-48*

4.1.16.1 dns-whitelist

dns-whitelist

Configures a DNS whitelist

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dns-whitelist <DNS-WHITELIST>
```

Parameters

<DNS-WHITELIST>	Enter the name of whitelist (will be created if it does not already exist)

Example

```
rfs7000-37FABE(config-dns-whitelist-test)#?
DNS Whitelist Mode commands:
  no        Negate a command or set its defaults
  permit    Match a host

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs7000-37FABE(config-dns-whitelist-test)#
```

4.1.16.2 dns-whitelist mode commands

Table 4.9 Summarizes dns-white-list mode commands

Table 4.9 *dns-whitelist commands*

Command	*Description*	*Reference*
permit	Matches a host	*page 4-50*
no	Negates a command or sets its default values	*page 4-51*

4.1.16.2.1 permit

dns-whitelist mode commands

A whitelist is a list of host names and IP addresses permitted access to the controller-managed network or captive portal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
permit <WORD> {suffix}
```

Parameters

<WORD> {suffix}	Permits a list of hostnames or IP addresses access to the controller managed network or hotspot • <WORD> – the host name or IP address of the device being permitted access. • suffix – Matches any hostname including the specified name as a suffix

Example

```
rfs7000-37FABE(config-dns-whitelist-test)#permit motorolasolutions.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#show context
dns-whitelist test
 permit motorolasolutions.com suffix
rfs7000-37FABE(config-dns-whitelist-test)#
```

4.1.16.2.2no

dns-whitelist mode commands

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no permit <WORD>
```

Parameters

no permit <WORD>	Does not match the hostname or IP address in the list and is not permitted access

Example

```
rfs7000-37FABE(config-dns-whitelist-test)#no permit motorolasolutions.com
rfs7000-37FABE(config-dns-whitelist-test)#
```

4.1.17 do

Global Configuration Commands

Runs commands from the EXEC mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
do <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the do command

Example

```
rfs7000-37FABE(config)#do ?
  ap-upgrade      AP firmware upgrade
  archive         Manage archive files
  boot            Boot commands
  cd              Change current directory
  change-passwd   Change password
  clear           Clear
  clock           Configure software system clock
  cluster         Cluster commands
  commit          Commit all changes made in this session
  configure       Enter configuration mode
  connect         Open a console connection to a remote device
  copy            Copy from one file to another
  crypto          Encryption related commands
  debug           Debugging functions
  delete          Deletes specified file from the system.
  diff            Display differences between two files
  dir             List files on a filesystem
  disable         Turn off privileged mode command
  edit            Edit a text file
  enable          Turn on privileged mode command
  erase           Erase a filesystem
  format          Format file system
  halt            Halt the system
  help            Description of the interactive help system
  logging         Modify message logging facilities
  mint            MiNT protocol
  mkdir           Create a directory
  more            Display the contents of a file
  no              Negate a command or set its defaults
  page            Toggle paging
  ping            Send ICMP echo messages
  pwd             Display current directory
  reload          Halt and perform a warm reboot
  remote-debug    Troubleshoot remote system(s)
  rename          Rename a file
  revert          Revert changes
  rmdir           Delete a directory
```

```
self            Config context of the device currently logged into
telnet          Open a telnet connection
terminal        Set terminal line parameters
time-it         Check how long a particular command took between request and
                completion of response
traceroute      Trace route to destination
upgrade         Upgrade software image
upgrade-abort   Abort an ongoing upgrade
watch           Repeat the specific CLI command at a periodic interval
write           Write running configuration to memory or terminal

clrscr          Clears the display screen
exit            Exit from the CLI
service         Service Commands
show            Show running system information
```

4.1.18 end

Global Configuration Commands

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to the previous mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
end
```

Parameters

None

Example

```
rfs7000-37FABE(config)#end
rfs7000-37FABE#
```

4.1.19 event-system-policy

Global Configuration Commands

Configures a policy which configures how events are handled by the wireless controller. Each event can be configured individually to perform an action such as sending an email or forwarding a notification to its parent controller etc.

Table 4.10 *Event System Policy Commands*

Command	Description	Reference
event-system-policy	Configures the event-system-policy.	page 4-56

4.1.19.1 event-system-policy

event-system-policy

Configures an event system policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
event-system-policy <EVENT-SYSTEM-POLICY>
```

Parameters

<EVENT-SYSTEM-POLICY>	Enter the name of event system policy (will be created if it does not already exist)

Example

```
rfs7000-37FABE(config)#event-system-policy event-testpolicy
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#?
Event System Policy Mode commands:
  event    Configure an event
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-event-system-policy-event-testpolicy)#
```

4.1.19.2 event-system-policy mode commands

event-system-policy

Table 4.11 Summarizes event system policy mode commands

Table 4.11 *event-system-policy mode commands*

Command	Description	Reference
event	Configures an event	*page 4-58*
no	Negates a command or sets its default values	*page 4-68*

4.1.19.2.1 event

event-system-policy mode commands

Configures an event

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
event [<event type>] [<event name>] [email|forward-to-switch|snmp|syslog]
[default|on|off]
```

NOTE: The parameter values for the <event type> and <event name> are summarized in the table under the Parameters section.

Parameters

<event type>	*<event name>*
aaa	• radius-discon-msg – RADIUS disconnection message • radius-session-expired – RADIUS session expired message • radius-session-not-started – RADIUS session not started message • radius-vlan-update – RADIUS VLAN update message
adv-wips	• adv-wips-event-1 – Event adv-wips-event-1 message • adv-wips-event-10 – Event adv-wips-event-10 message • adv-wips-event-105 – Event adv-wips-event-105 message • adv-wips-event-109 – Event adv-wips-event-109 message • adv-wips-event-11 – Event adv-wips-event-11 message • adv-wips-event-110 – Event adv-wips-event-110 message • adv-wips-event-111 – Event adv-wips-event-111 message • adv-wips-event-112 – Event adv-wips-event-112 message • adv-wips-event-113 – Event adv-wips-event-113 message • adv-wips-event-114 – Event adv-wips-event-114 message • adv-wips-event-115 – Event adv-wips-event-115 message • adv-wips-event-116 – Event adv-wips-event-116 message • adv-wips-event-117 – Event adv-wips-event-117 message • adv-wips-event-118 – Event adv-wips-event-118 message • adv-wips-event-119 – Event adv-wips-event-119 message • adv-wips-event-12 – Event adv-wips-event-12 message • adv-wips-event-120 – Event adv-wips-event-120 message • adv-wips-event-121 – Event adv-wips-event-121 message • adv-wips-event-13 – Event adv-wips-event-13 message • adv-wips-event-14 – Event adv-wips-event-14 message • adv-wips-event-142 – Event adv-wips-event-142 message • adv-wips-event-16 – Event adv-wips-event-16 message • adv-wips-event-19 – Event adv-wips-event-19 message • adv-wips-event-2 – Event adv-wips-event-2 message • adv-wips-event-21 – Event adv-wips-event-21message • adv-wips-event-220 – Event adv-wips-event-220 message
	• adv-wips-event-221 – Event adv-wips-event-221 message • adv-wips-event-222 – Event adv-wips-event-222 message • adv-wips-event-25 – Event adv-wips-event-25 message • adv-wips-event-26 – Event adv-wips-event-26 message • adv-wips-event-29 – Event adv-wips-event-29 message • adv-wips-event-3 – Event adv-wips-event-3 message • adv-wips-event-47 – Event adv-wips-event-47 message • adv-wips-event-63 – Event adv-wips-event-63 message • adv-wips-event-87 – Event adv-wips-event-87 message

<event type>	*<event name>*
ap	• adopted – Event adopted message • adopted-to-controller – Event adopted to controller message • ap-autoup-done – Event ap autoup done message • ap-autoup-fail – Event ap autoup fail message • ap-autoup-needed – Event ap autoup needed message • ap-autoup-no-need – Event ap autoup not needed message • ap-autoup-reboot – Event ap autoup reboot message • ap-autoup-timeout – Event ap autoup timeout message • ap-autoup-ver – Event ap autoup version message • image-parse-failure – Event image parse failure message • legacy-auto-update – Event legacy auto update message • no-image-file – Event no image file message • reset – Event reset message • sw-conn-lost – Event software connection lost message • unadopted – Event unadopted message
captive-portal	• allow-access – Event allow access message • auth-failed – Event authentication failed message • auth-success – Event authentication success message • client-disconnect – Event client disconnected message • client-removed – Event client removed message • flex-log-access – Event flexible log access message • inactivity-timeout – Event inactivity timeout message • purge-client – Event purge client message • session-timeout – Event session timeout message

<event type>	*<event name>*
certmgr	• ca-cert-actions-failure – Event ca certificate actions failure message • ca-cert-actions-success – Event ca certificate actions success message • ca-key-actions-failure – Event ca key actions failure message • ca-key-actions-success – Event ca key actions success message • cert-expiry – Event certificate expiry message • crl-actions-failure – Event crl (Certificate Revocation List) actions failure message • crl-actions-success – Event crl (Certificate Revocation List) actions success message • csr-export-failure – Event csr (Certificate Server Request) export failure message • csr-export-success – Event csr (Certificate Server Request) export success message • delete-trustpoint-action – Event delete trustpoint action message • export-trustpoint – Event export trustpoint message • import-trustpoint – Event import trustpoint message • rsa-key-actions-failure – Event RSA key actions failure message • rsa-key-actions-success – Event RSA key actions success message • srv-cert-actions-success – Event server certificate actions success message • svr-cert-actions-failure – Event server certificate actions failure message
cfgd	• acl-attached-altered – Event acl attached altered message • acl-rule-altered – Event acl rule altered message
cluster	• max-exceeded – Event maximum exceeded message
crm	Event Critical Resource Monitoring • critical-resource-down – Event Critical Resource Down • critical-resource-up – Event Critical Resource Up
dhcpsvr	• dhcp-start • dhcpsvr-stop – Event DHCP sever stopped • relayifacenoip – Event relay interface no IP message • relaynoiface – Event relay no interface message • relay-start – Event relay agent started • relay-stop – Event DHCP relay agent stopped

<event type>	*<event name>*
diag	• autogen-tech-sprt – Event autogen technical support message • buf-usage – Event buffer usage message • cpu-load – Event CPU load message • disk-usage – Event disk usage message • elapsed-time – Event elapsed time message • fan-underspeed – Event fan underspeed message • fd-count – Event forward count message • free-flash-disk – Event free flash disk message • free-flash-inodes – Event free flash inodes message • free-nvram-disk – Event free nvram disk message • free-nvram-inodes – Event free nvram inodes message • free-ram – Event free ram message • free-ram-disk – Event free ram disk message • free-ram-inodes – Event free ram inodes message • head-cache-usage – Event head cache usage message • high-temp – Event high temp message • ip-dest-usage – Event ip destination usage message • led-identify – Event led identify message • low-temp – Event low temp message • new-led-state – Event new led state message • over-temp – Event over temp message • over-voltage – Event over voltage message • poe-init-fail – Event PoE init fail message • poe-power-level – Event PoE power level message • poe-read-fail – Event PoE read fail message • poe-state-change – Event PoE state change message • ram-usage – Event ram usage message • under-voltage – Event under voltage message • wd-reset-sys – Event wd reset system message • wd-state-change – Event wd state change message

<event type>	*<event name>*
dot11	• client-associated – Wireless client associated event message • client-denied-assoc – Event client denied association message • client-disassociated – Wireless client disassociated message • country-code – Event country code message • country-code-error – Event country code error message • eap-cached-keys – Event EAP cached keys message • eap-client-timeout – Event EAP client timeout message • eap-failed – Event EAP failed message • eap-opp-cached-keys – Event EAP opp cached keys message • eap-preauth-client-timeout – Event eap preauthentication client timeout message • eap-preauth-failed – Event EAP preauthentication failed message • eap-preauth-server-timeout – Event EAP preauthentication server timeout message • eap-preauth-success – Event EAP preauthentication success message • eap-server-timeout – Event EAP server timeout message • eap-success – Event EAP success message • kerberos-client-failed – Event kerberos client failed message • kerberos-client-success – Event kerberos client success message • kerberos-wlan-failed – Event kerberos WLAN failed message • kerberos-wlan-success – Event kerberos WLAN success message • kerberos-wlan-timeout – Event kerberos WLAN timeout message • tkip-cntrmeas-end – Event TKIP cntrmeas end message • tkip-cntrmeas-start – Event TKIP cntrmeas start message • tkip-mic-fail-report – Event TKIP mic fail report message • tkip-mic-failure – Event TKIP mic failure message • unsanctioned-ap-active – Event unsanctioned AP active message • unsanctioned-ap-inactive – Event unsanctioned AP inactive message • unsanctioned-ap-status-change – Event unsanctioned AP status change • voice-call-completed – Event voice call completed message • voice-call-failed – Event voice call failed message • wpa-wpa2-failed – Event WPA-WPA2 failed message • wpa-wpa2-key-rotn – Event WPA-WPA2 key rotn message • wpa-wpa2-success – Event WPA-WPA2 success message

<event type>	*<event name>*
filemgmt	• http – Event HTTP message • httplocal – Event HTTP local message • https-start – Event HTTPS start message • https-wait – Event HTTPS wait message • httpstart – Event HTTP start message • keyadded – Event key added message • keydeleted – Event key deleted message • trustpointdeleted – Event trustpoint deleted message
fwu	• fwuaborted – Event fwu aborted message • fwubadconfig – Event fwu bad config message • fwucorruptedfile – Event fwu corrupted file message • fwucouldntgetfile – Event fwu could not get file message • fwudone – Event fwu done message • fwufileundef – Event fwu file undefined message • fwunoneed – Event fwu no need message • fwuprodmismatch – Event fwu prod mismatch message • fwuserverundef – Event fwu server undefined message • fwuserverunreachable – Event fwu server unreachable message • fwusignmismatch – Event fwu signature mismatch message • fwusyserr – Event fwu system error message • fwuunsupportedhw – Event fwu unsupported hardware message • fwuvermismatch – Event fwu version mismatch message
licmgr	• licbaddata – Event license bad data message • licbadfeature – Event license bad feature message • licbadproduct – Event license bad product message • licexpired – Event license expired message • licincompdata – Event license incomplete data message • licmodified – Event license modified message • newlicense – Event new license message
mesh	• mesh-link-down – Event mesh link down message • mesh-link-up – Event mesh link up message
nsm	• dhcpc-err – Event DHCP certification error message • dhcpdefrt – Event DHCP defrt message • dhcpip – Event DHCP IP message • dhcpipchg – Event DHCP IP change message • dhcpipnoadd – Event DHCP IP no add message • dhcpnodefrt – Event DHCP no defrt message • ifdown – Event if down message • ifipcfg – Event if IP config message • ifup – Event If up message

<event type>	*<event name>*
pm	• procid – Event procid message • procmaxrstrt – Event proc max restart message • procnoresp – Event proc no response message • procrstrt – Event proc restart message • procstart – Event proc start message • procstop – Event proc stop message • procsysrstrt – Event proc system restart message • startupcomplete – Event startup complete message
radconf	raduserpassstrength – Event RADIUS user pass strength message
radio	• radar-detected – Event radar detected message • radar-scan-completed – Event radar scan completed message • radar-scan-started – Event radar scan started message • radio-state-change – Event radio state change message • resume-home-channel – Event resume home channel message
rns	• adaptererr – Event adapter error message • adapterstatechange – Event adapter state change message • adapterstatus – Event adapter status message • adaptertag – Event adapter tag message • alelicensemissing –Event ale license missing message • devicestatechange – Event device state change message • taglocation – Event tag location message
securitymgr	• deprecatedcli – Event deprecated cli message • fatal-hit – Event fatal hit message • log-cli-error – Event log cli error message • userpassstrength – Event user pass strength message
smrt	• calibration-done – Event calibration done message • calibration-started – Event calibration started message • config-cleared – Configuration cleared event message • cov-hole-recovery – Event coverage hole recovery message • cov-hole-recovery-done – Event coverage hole recovery done message • interference-recovery – Event interference recovery message • neighbor-recovery – Event neighbor recovery message • power-adjustment – Event power adjustment message

<event type>	*<event name>*
smtpnot	• cfg – Event cfg message • cfginc – Event cfg inc message • net – Event net message • proto – Event proto message • smtpauth – Event SMTP authentication message • smtperr – Event SMTP error message • smtpinfo – Event SMTP information message
system	• clock-reset – Event clock reset message • http – Event HTTP message • login – Event login message • login-fail – Event login fail message • login-fail-access – Event login fail access message • login-fail-bad-role – Event login fail bad role message • logout – Event logout message • panic – Event panic message • procstop – Event proc stop message • system-autoup-disable – Event system autoup disable message • system-autoup-enable – Event system autoup enable message • ui-user-auth-fail – Event ui user authentication fail message • ui-user-auth-success – Event ui user authentication success message
test	• testalert – Event test alert message • testargs – Event test arguments message • testcrit – Event test critical message • testdebug – Event test debug message • testemerg – Event test emergency message • testerr – Event test error message • testinfo – Event test information message • testnotice – Event test notice message • testwarn – Event test warning message
wips	• wips-client-blacklisted – Event WIPS client blacklisted message • wips-client-rem-blacklist – Event WIPS client rem blacklist message • wips-event – Event WIPS event

email	Email notifications
forward-to-switch	Forward
snmp	SNMP
syslog	Syslog
default	Default

off	Off
on	On

Example

```
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#event aaa radius-discon-
msg email on forward-to-switch default snmp default syslog default
rfs7000-37FABE(config-event-system-policy-event-testpolicy)#

rfs7000-37FABE(config-event-system-policy-adv-wips)#


rfs7000-37FABE(config-event-system-policy-testpolicy)#show context
event-system-policy testpolicy
 event sole adaptererr syslog off snmp off forward-to-switch off
rfs7000-37FABE(config-event-system-policy-testpolicy)#
```

4.1.19.2.2no

event-system-policy mode commands

Negates an event configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [<event type>] [<event name>] [email|forward-to-switch|snmp|syslog]
[default|on|off]
```

Parameters

None

Example

```
rfs7000-37FABE(config-event-system-policy-testpolicy)#

rfs7000-37FABE(config-event-system-policy-testpolicy)#no event aaa
% Error: event_system_policy[aaa] does not exist, unable to delete
rfs7000-37FABE(config)#
```

4.1.20 firewall-policy

Global Configuration Commands

Configures a firewall policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
firewall-policy <firewall-policy-name>
```

Parameters

<firewall-policy-name>	Enter a firewall policy name to configure

Example

```
rfs7000-37FABE(config)#firewall-policy test
rfs7000-37FABE(config-fw-policy-test)#
```

NOTE: For more information, see Chapter 14, FIREWALL-POLICY.

4.1.21 help

Global Configuration Commands

Describes the interactive help system.

Use this command to access the advanced help feature. Use "**?**" anytime at the command prompt to access a help topic.

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
help {search} <WORD> {detailed|only-show|skip-show}
```

Parameters

{search} <WORD> {detailed|only-show|skip-show}	Searches for CLI commands related to a specific term • <WORD> – Enter a term to search CLI commands (Eg: a feature or a configuration parameter) • detailed – Searches and displays help strings in addition to mode and commands • only-show – Displays only "show" commands, not configuration commands • skip-show – Displays only configuration commands, not "show" commands

Example

```
Mode    : Priv Exec
Command : show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))
           \ Show running system information
            \ Debugging functions
             \ Wireless Module
              \ On AP/Controller or RF-Domain
               \ AP / Controller / RF-Domain name

        : show adoption info (|(on DEVICE-NAME))
              \ Show running system information
              \ Display information related to adoption to wireless controller
              \ Display adoption status of this device and its adopted access point
              \ On AP/Controller
              \ AP / Controller name

        : show adoption offline
              \ Show running system information
              \ Display all information related to unadopted to wireless controller
             \ Display unadopted status of this device and its adopted access point
```

```
        : show wireless ap (|(on DEVICE-OR-DOMAIN-NAME))
              \ Show running system information
              \ Wireless commands
              \ Information regarding managed Access Points
              \ On AP/Controller or RF-Domain
              \ AP / Controller / RF-Domain name

        : show wireless ap configured
              \ Show running system information
              \ Wireless commands
              \ Information regarding managed Access Points
              \ Information of all Access Points in configuration

        : show wireless ap detail (|WORD)
              \ Show running system information
              \ Wireless commands
              \ Information regarding managed Access Points
              \ detailed information for given AP
              \ AP mac address or its hostname

        : show wireless unsanctioned aps (|(on DEVICE-OR-DOMAIN-NAME))
              \ Show running system information
--More--
rfs7000-37FABE(config)#
```

4.1.22 host

Global Configuration Commands

Enters the configuration context of a remote device using its hostname.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
host <DEVICE-NAME>
```

Parameters

<DEVICE-NAME>	The name of the controller. This name is displayed when the controller is accessed from any network.

Example

```
rfs7000-37FABE(config)#host
rfs7000-37FAAA                    RFDOMAIN_UseCase1/rfs7000-37FAAA
rfs7000-37FABE(config)#host RFDOMAIN_UseCase1/rfs7000-37FAAA
rfs7000-37FABE(config-device-00-15-70-37-FA-AA)#
```

4.1.23 igmp-snoop-policy

Global Configuration Commands

Configures an igmp-snoop policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
igmp-snoop-policy <igmp-snoop-policy -name>
```

Parameters

<igmp-snoop-policy-name>	Enter a igmp-snoop policy name to configure

Example

```
rfs7000-37FABE(config)#igmp-snoop-policy test
rfs7000-37FABE(config)#?
```

NOTE: For more information, see Chapter 15, IGMP-SNOOP-POLICY.

4.1.24 ip

Global Configuration Commands

Configures a selected *Internet Protocol* (IP) component

Access-lists define access to the controller managed network using a set of rules. Each rule specifies an action taken when a packet matches a given set of rules. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. The controller supports the following ACLs:

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip access-list <IP-ACCESS-LIST>
```

Parameters

access-list <IP-ACCESS-LIST>	Configures an access-list • <IP-ACCESS-LIST> – Enter the name of the ACL to configure

Example

```
rfs7000-37FABE(config)#ip access-list test
rfs7000-37FABE(config-ip-acl-test)#
```

NOTE: For more information, see Chapter 12, ACCESS-LIST.

4.1.25 mac

Global Configuration Commands

Configures MAC access lists (goes to the MAC ACL mode)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mac access-list <MAC-ACCESS-LIST>
```

Parameters

access-list <MAC-ACCESS-LIST>	Defines the ACL configuration for the MAC address • <MAC-ACCESS-LIST> – Defines the name of the ACL

Usage Guidelines

To delete MAC ACL, use **no access-list <access-list name>** under the Global Config mode.

Example

```
rfs7000-37FABE(config)#mac access-list test1
rfs7000-37FABE(config)#
```

NOTE: When using the **mac access-list** parameter, enter the following contexts:

```
rfs7000-37FABE(config)#mac  access-list <access-list-
name>
rfs7000-37FABE(config-mac-acl-test1)#
```

For more information, see Chapter 12, ACCESS-LIST.

4.1.26 management-policy

Global Configuration Commands

Configures a management policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
management-policy <management-policy-name>
```

Parameters

<management-policy-name>	Enter a management policy name to configure

Example

```
rfs7000-37FABE(config)#management-policy test
rfs7000-37FABE(config-management-policy-test)#
```

NOTE: For more information, see Chapter 17, MANAGEMENT-POLICY.

4.1.27 mint-policy

Global Configuration Commands

Configures the global MiNT policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mint-policy global-default
```

Parameters

<mint-policy-name>	Enter a MiNT policy name to configure

Example

```
rfs7000-37FABE(config)#mint-policy global-default
rfs7000-37FABE(config-mint-policy-global-default)#
```

NOTE: For more information, see Chapter 16, MINT-POLICY.

4.1.28 nac-list

Global Configuration Commands

Configures a policy which configures a list of devices that can access a wireless controller managed network based on their MAC addresses.

Table 4.12 *NAC List Commands*

Command	Description	Reference
nac-list	Creates a nac-list policy.	page 4-79

4.1.28.1 nac-list

Global Configuration Commands

Configures a network access control list that controls access to the wireless controller managed network.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
nac-list <NAC-LIST>
```

Parameters

<NAC-LIST>	Enter the name of the nac-list to be configured

Example

```
rfs7000-37FABE(config)#nac test
rfs7000-37FABE(config-nac-list-test)#?
NAC List Mode commands:
  exclude  Specify MAC addresses to be excluded from the NAC enforcement list
  include  Specify MAC addresses to be included in the NAC enforcement list
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-nac-list-test)#
```

4.1.28.2 nac-list-mode

Table 4.13 Summarizes nac-list mode commands

Table 4.13 *nac-list-mode commands*

Command	Description	Reference
exclude	Specifies the MAC addresses excluded from the NAC enforcement list	*page 4-81*
include	Specifies the MAC addresses included from the NAC enforcement list	*page 4-82*
no	Negates a command or sets its default values	*page 4-83*

4.1.28.2.1 exclude

nac-list-mode

Specifies the MAC addresses to be excluded from the NAC enforcement list

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
exclude <Start-MAC> [<End-MAC> precedence <1-1000>|precedence <1-1000>]
```

Parameters

<Start-MAC> [<End-MAC> precedence <1-1000>|precedence <1-1000>]	Enter the starting MAC address of a range of MACs excluded from the NAC enforcement list • <End-MAC> – Enter the ending MAC address of a range of MACs. It is optional if a single mac address has to be added • precedence <1-1000> – Enter a rule precedence value from <1-1000>. The rules are verified in an increasing order of precedence • precedence <1-1000> – Enter a rule precedence value from <1-1000>. The rules are verified in an increasing order of precedence

Example

```
rfs7000-37FABE(config-nac-list-test)#exclude 00-40-96-B0-BA-2A precedence 1
rfs7000-37FABE(config-nac-list-test)#
```

4.1.28.2.2include

nac-list-mode

Specifies the MAC addresses included in the NAC enforcement list

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
include <Start-MAC> [<End-MAC> precedence <1-1000>|precedence <1-1000>]
```

Parameters

<Start-MAC> [<End-MAC> precedence <1-1000>|precedence <1-1000>]	Enter the starting MAC address of a range of MACs included in the NAC enforcement list • <End-MAC> – Enter the ending MAC address of a range of MACs. It is optional if a single MAC address has to be added • precedence <1-1000> – Enter a rule precedence value from <1-1000>. The rules are verified in an increasing order of precedence • precedence <1-1000> – Enter a rule precedence value from <1-1000>. The rules are verified in an increasing order of precedence

Example

```
rfs7000-37FABE(config-nac-list-test)#include 00-40-96-B0-BA-2A precedence 1
rfs7000-37FABE(config-nac-list-test)#
```

4.1.28.2.3no

nac-list-mode

Negates including or excluding a rule command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [exclude|include]
```

Parameters

exclude	Enter an exclude rule to be deleted
include	Enter an include rule to be deleted

Example

```
rfs7000-37FABE(config-nac-list-test)#no include 00-40-96-B0-BA-2A precedence 1
rfs7000-37FABE(config-nac-list-test)#show context
nac-list test
rfs7000-37FABE(config-nac-list-test)#
```

4.1.29 no

Global Configuration Commands

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no <parameter>
```

Parameters

None

Example

```
rfs7000-37FABE(config)#no ?
  aaa-policy                Delete a aaa policy
  advanced-wips-policy      Delete an advanced-wips policy
  ap650                     Delete an AP650 access point
  ap6511                    Delete an AP6511 access point
  ap6532                    Delete an AP6532 access point
  ap71xx                    Delete an AP71XX access point
  association-acl-policy    Delete an association-acl policy
  auto-provisioning-policy  Delete an auto-provisioning policy
  captive-portal            Delete a captive portal
  critical-resource-policy  Remove device onboard critical resource policy
  customize                 Restore the custom cli commands to default
  device                    Delete multiple devices
  device-categorization     Delete  device categorization object
  dhcp-server-policy        DHCP server policy
  dns-whitelist             Delete a whitelist object
  event-system-policy       Delete a event system policy
  firewall-policy           Configure firewall policy
  igmp-snoop-policy         Remove device onboard igmp snoop policy
  ip                        Internet Protocol (IP)
  mac                       MAC configuration
  management-policy         Delete a management policy
  nac-list                  Delete an network access control list
  password-encryption       Disable password encryption in configuration
  profile                   Delete a profile and all its associated
                            configuration
  radio-qos-policy          Delete a radio QoS configuration policy
  radius-group              Local radius server group configuration
  radius-server-policy      Remove device onboard radius policy
  radius-user-pool-policy   Configure Radius User Pool
  rf-domain                 Delete one or more RF-domains and all their
                            associated configurations
  rfs4000                   Delete an RFS4000 wireless controller
  rfs6000                   Delete an RFS6000 wireless controller
  rfs7000                   Delete an RFS7000 wireless controller
  role-policy               Role based firewall policy
  smart-rf-policy           Delete a smart-rf-policy
  wips-policy               Delete a wips policy
  wlan                      Delete a wlan object
  wlan-qos-policy           Delete a wireless lan QoS configuration policy
```

```
service                     Service Commands
```

4.1.30 password-encryption

Global Configuration Commands

Enables password encryption with in a configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
password-encryption secret 2 <LINE>
```

Parameters

secret 2 <LINE>	Encrypts the passwords with secret phrase • 2 – Specifies the type of encryption as either SHA256 or AES256 • <LINE> – Enter the passphrase used for encryption

Example

```
rfs7000-37FABE(config)#password-encryption secret 2 symbol
rfs7000-37FABE(config)#
```

4.1.31 profile

Global Configuration Commands

Configures profile related commands. If no parameters are given, all the profiles are selected

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
profile {ap650|ap6511|ap6532|ap71xx|containing|filter|rfs4000|rfs6000|
rfs7000}
profile containing <WORD> {filter} type [ap6511|ap6531|ap7131|rfs4000|
   rfs6000|rfs7000]
profile filter type [ap6511|ap6531|ap7131|rfs4000|rfs6000|rfs7000]
```

Parameters

{ap650|ap6511| ap6532|ap7131| containing|filter|rfs4000| rfs6000|rfs7000}	• containing <WORD> – Specifies the profiles that contain a sub-string in the host-name
	  • <WORD> – Specify a substring in the profile name to filter the profiles
	• filter type – Specify the additional selection filter by profile type from the list of profiles
	  • ap650 – AP650 access point profile
	  • ap6511 – AP6511 access point profile
	  • ap6532 – AP6532 access point profile
	  • ap71xx– AP71xx access point profile
	  • rfs4000 – RFS4000 wireless controller profile
	  • rfs6000 – RFS6000 wireless controller profile
	  • rfs7000 – RFS7000 wireless controller profile

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#?
Profile Mode commands:
  aaa                             VPN AAA authentication settings
  ap-upgrade                      AP firmware upgrade
  arp                             Static Address Resolution Protocol (ARP)
  autoinstall                     Autoinstall Configuration commands
  automatic-write                 Enable automatic write of startup
                                  configuration file
  bridge                          Ethernet bridge
  cdp                             Cisco Discovery Protocol
  cluster                         Cluster configuration
  controller                      Add controller
  controller-group                Controller group this controller belongs to
  crypto                          Encryption related commands
  dscp-mapping                    Configure IP DSCP to 802.1p priority mapping
                                  for untagged frames
  events                          System event messages
  interface                       Select an interface to configure
  ip                              Internet Protocol (IP)
```

```
  led                                Turn LEDs on/off on the device
  legacy-auto-update                 Enable legacy device firmware auto update
  lldp                               Link Layer Discovery Protocol
  load-balancing                     Configure load balancing parameter
  local                              Local user authentication database for VPN
  logging                            Modify message logging facilities
  mac-address-table                  MAC Address Table
  mint                               MiNT protocol
  misconfiguration-recovery-time     Check controller connectivity after
                                     configuration is received
  monitor                            Critical resource monitoring
  no                                 Negate a command or set its defaults
  noc                                Configure the noc related setting
  ntp                                Ntp server A.B.C.D
  power-config                       Configure power mode
  preferred-controller-group         Controller group this system will prefer for
                                     adoption
  radius                             Configure device-level radius authentication
                                     parameters
  rf-domain-manager                  RF Domain Manager
  spanning-tree                      Spanning tree
  use                                Set setting to use
  vpn                                Vpn configuration
  wep-shared-key-auth                Enable support for 802.11 WEP shared key
                                     authentication

  clrscr                             Clears the display screen
  commit                             Commit all changes made in this session
  do                                 Run commands from Exec mode
  end                                End current mode and change to EXEC mode
  exit                               End current mode and down to previous mode
  help                               Description of the interactive help system
  revert                             Revert changes
-------------------------------------------------------------------------------
-------------------------------------------------------------rfs7000-
37FABE(config-profile-default-rfs7000)#
```

NOTE: For more information, see Chapter 7, PROFILES.

4.1.32 radio-qos-policy

Global Configuration Commands

Configures a radio quality of service policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
radio-qos-policy <radio-qos-policy-name>
```

Parameters

<radio-qos-policy-name>	Enter the name of the QoS policy

Example

```
rfs7000-37FABE(config)#radio-qos-policy test
rfs7000-37FABE(config)#
```

NOTE: For more information, see Chapter 19, RADIO-QOS-POLICY.

4.1.33 radius-group

Global Configuration Commands

Configures RADIUS user group parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
radius-group <radius-group-name>
```

Parameters

<radius-group-name>	Enter a user group name up to 64 characters

Example

```
rfs7000-37FABE(config)#radius-group testgroup
rfs7000-37FABE(config)#
```

NOTE: For more information, see Chapter 18, RADIUS-POLICY.

4.1.34 radius-server-policy

Global Configuration Commands

Creates an onboard device RADIUS policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
radius-server-policy <radius-server-policy-name>
```

Parameters

<radius-server-policy-name>	Enter a RADIUS server policy name

Example

```
rfs7000-37FABE(config)#radius-server-policy testpolicy
rfs7000-37FABE(config)#
```

NOTE: For more information, see Chapter 18, RADIUS-POLICY.

4.1.35 radius-user-pool-policy

Global Configuration Commands

Configures a RADIUS user pool

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
radius-user-pool-policy <radius-user-pool-policy-name>
```

Parameters

<radius-user-pool-policy>	Enter the radius-user-pool-policy name

Example

```
rfs7000-37FABE(config)#radius-user-pool-policy testpool
rfs7000-37FABE(config)#
```

NOTE: For more information, see Chapter 18, RADIUS-POLICY.

4.1.36 rf-domain

Global Configuration Commands

RF Domain groups devices that can logically belong to one network. The rf-domain policy configures a set of parameters that enable devices to be configured quickly as belonging to a particular RF domain.

Table 4.14 *RF Domain Commands*

Command	Description	Reference
rf-domain	Creates a rf-domain policy.	page 4-94

4.1.36.1 rf-domain

rf-domain

Creates a RF Domain configuration. If the policy does not exist, it creates a new policy.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`rf-domain {RF-DOMAIN|containing <WORD>}`

Parameters

{RF-DOMAIN|containing <WORD>}	Defines the name of a RF Domain • containing <WORD> – Specify domains that contain a sub-string in the domain name

Example

```
rfs7000-37FABE(config)#rf-domain rfs7000
rfs7000-37FABE(config-rf-domain-rfs7000)#

rfs4000-880DA7(config)#rf-domain default
rfs4000-880DA7(config-rf-domain-default)#
```

4.1.36.2 rf-domain-mode

rf-domain

This section describes the default commands under rf-domain.

Table 4.15 Summarises rf-domain commands

Table 4.15 *rf-domain Commands*

Command	Description	Reference
channel-list	Configures channel list advertised by radios	*page 4-96*
control-vlan	Configures VLAN for traffic control on the RF Domain	*page 4-97*
layout	Configures layout information	*page 4-98*

4.1.36.2.1 channel-list

rf-domain-mode

Configures channel list advertised by radios

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
channel-list [2.4GHz|5GHz|dynamic]
channel-list [2.4GHz|5GHz] <WORD>
```

Parameters

[2.4GHz|5GHz|dynamic]	• 2.4GHz <WORD> – Configures the channel list advertised by radios operating in 2.4GHz mode • 5GHz <WORD> – Configures the channel list advertised by radios operating in 5GHz mode • dynamic – Enables dynamic update of configured channel-list

Example

```
rfs7000-37FABE(config-rf-domain-default)#channel-list 2.4GHz 1-10
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain RFDOMAIN_UseCase1
 location SanJose
 contact txyr399@motorola-solutions.com
 timezone America/Los_Angeles
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
rfs7000-37FABE(config-rf-domain-default)#
```

4.1.36.2.2control-vlan

rf-domain-mode

Configures VLAN for traffic control on the RF Domain

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
control-vlan <1-4094>
```

Parameters

<1-4094>	Configures VLAN ID between 1 and 4094

Example

```
rfs7000-37FABE(config-rf-domain-default)#control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain RFDOMAIN_UseCase1
 location SanJose
 contact txyr399@motorola-solutions.com
 timezone America/Los_Angeles
 country-code us
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 control-vlan 1
rfs7000-37FABE(config-rf-domain-default)#
```

4.1.36.2.3layout

rf-domain-mode

Configure layout maps for every rf-domain/floor/area. It allows users to place APs across the deployment map. A maximum of 256 layouts will be permitted.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
layout map-location <WORD> units [feet|meters] {area|floor} <WORD>
```

Parameters

map-location <WORD> units [feet|meters] {area |floor} <WORD>	• map-location <WORD> – Configures map-location for the layout • <WORD> – Specify the URL to configure • units [feet|meters] – Configures map units in terms of feet/meters • feet – Specify the measurement in feet • meters – Specify the measurement in meters • {area <WORD> – Configures area name for the layout • floor <WORD> – Configures floor name for the layout

Example

```
rfs7000-37FABE(config-rf-domain-default)#layout map-location www.firstfloor.com
units meters area Ecospace floor Floor5
rfs7000-37FABE(config-rf-domain-default)#

rfs7000-37FABE(config-rf-domain-default)#show context
rf-domain default
 country-code us
 sensor-server 1 ip 172.16.10.14 port 1
 channel-list dynamic
 channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
 layout map-location www.firstfloor.com units meters area Ecospace floor Floor5
rfs7000-37FABE(config-rf-domain-default)#
```

NOTE: The remaining commands under rf-domain are same as Device-Mode Commands. For more information, see Chapter 7, Device Specific Commands.

4.1.37 rfs4000

Global Configuration Commands

Adds an RFS4000 controller to the network

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rfs4000 <DEVICE-RFS4000>
```

Parameters

<DEVICE-RFS4000>	Enter MAC address of a RFS4000

Example

```
rfs7000-37FABE(config)#rfs4000 10-20-30-40-50-60
rfs7000-37FABE(config-device-10-20-30-40-50-60)#
```

4.1.38 rfs6000

Global Configuration Commands

Adds an RFS6000 controller to the network

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rfs6000 <DEVICE-RFS6000>
```

Parameters

<DEVICE-RFS6000>	Enter the MAC address of a RFS6000

Example

```
rfs7000-37FABE(config)#rfs6000 11-20-30-40-50-61
rfs7000-37FABE(config-device-11-20-30-40-50-61)#
```

4.1.39 rfs7000

Global Configuration Commands

Adds an RFS7000 controller to the network

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rfs7000 <DEVICE-RFS7000>
```

Parameters

<DEVICE-RFS7000>	Enter the MAC address of a RFS7000

Example

```
rfs7000-37FABE(config)#rfs7000 12-20-30-40-50-62
rfs7000-37FABE(config-device-12-20-30-40-50-62)#
```

4.1.40 role-policy

Global Configuration Commands

Configures a role based firewall policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
role-policy <role-policy-name>
```

Parameters

<role-policy>	Enter the role-policy name to configure

Example

```
rfs7000-37FABE(config)#role-policy role1
rfs7000-37FABE(config)#
```

NOTE: For more information, see Chapter 20, ROLE-POLICY.

4.1.41 self

Global Configuration Commands

Displays the configuration context of the currently logged device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
self
```

Parameters

None

Example

```
rfs7000-37FABE(config)#self
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

4.1.42 service

Global Configuration Commands

Retrieves system data (tables, log files, configuration, status and operation) for debugging and problem resolution

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
service [set|show cli]
service set [command-history <10-300>|reboot-history <10-100>|
upgrade-history <10-100>] {on <DEVICE-NAME>}
```

Parameters

set [command-history <10-300>|reboot-history <10-100>|upgrade-history <10-100>] {on <DEVICE-NAME>}	Sets service parameters
	• command-history <10-300> – Set the command history size between 10 and 300. The default size is 200
	• reboot-history <10-100> – Set the reboot history size between 10 and 100. The default size is 50
	• upgrade-history <10-100> – Set the upgrade history size between 10 and 100. The default size is 50
	  • {on <DEVICE-NAME>} – Optional. Displays the AP/Controller
	  • <DEVICE-NAME> – AP/Controller name

show cli	Displays running system information • cli – Displays the CLI tree of the current mode

Example

```
rfs7000-37FABE(config)#service show cli
Global Config mode:
+-line
  +-console
    +-<0-0> [line console <0-0>]
  +-vty
    +-<0-871> [line vty <0-871> (<0-871>|)]
      +-<0-871> [line vty <0-871> (<0-871>|)]
+-help [help]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show)]
      +-detailed [help search WORD (|detailed|only-show|skip-show)]
      +-only-show [help search WORD (|detailed|only-show|skip-show)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show)]
+-show
  +-commands [show commands]
  +-running-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config) (|include-factory)]
    +-interface [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-
4094>') (|include-factory)]
      +-WORD [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-
4094>') (|include-factory)]
```

```
        +-include-factory [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-
4>|vlan <1-4094>') (|include-factory)]
      +-ge
        +-<1-4> [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-
4094>') (|include-factory)]
         +-include-factory [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-
4>|vlan <1-4094>') (|include-factory)]
      +-me1 [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-
4094>') (|include-factory)]
        +-include-factory [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-
4>|vlan <1-4094>.....................................................................
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#service set reboot-history 50
rfs7000-37FABE(config)#
```

4.1.43 show

Global Configuration Commands

Displays running system information under various parameters such as, auto-provisioning-policy, advanced-wips policy and boot configuration details.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show <parameter>
```

Parameters

None

NOTE: For more information, see Chapter 6, SHOW COMMANDS.

Example

```
rfs7000-37FABE(config)#show ?
 adoption                Display information related to adoption to wireless
                          controller
  advanced-wips          Advanced WIPS
  ap-upgrade             AP Upgrade
  boot                   Display boot configuration.
  captive-portal         Captive portal commands
  cdp                    Cisco Discovery Protocol
  clock                  Display system clock
  cluster                Cluster Protocol
  commands               Show command lists
  context                Information about current context
  critical-resources     Critical Resources
  crypto                 Encryption related commands
  debug                  Debugging functions
  debugging              Debugging functions
  device-categorization  Device Categorization
  event-history          Display event history
  event-system-policy    Display event system policy
  file                   Display filesystem information
  firewall               Wireless Firewall
  interface              Interface Configuration/Statistics commands
  ip                     Internet Protocol (IP)
  ip-access-list-stats   IP Access list stats
  licenses               Show installed licenses and usage
  lldp                   Link Layer Discovery Protocol
  mac-access-list-stats  MAC Access list stats
  mac-address-table      Display MAC address table
  mint                   MiNT protocol
  noc                    Noc-level information
  ntp                    Network time protocol
  password-encryption    Pasword encryption
```

```
  power                    Show power over ethernet command
  remote-debug             Show details of remote debug sessions
  rf-domain-manager        Show RF Domain Manager selection details
  role                     Role based firewall
  running-config           Current operating configuration
  session-changes          Configuration changes made in this session
  session-config           This session configuration
  sessions                 Display CLI sessions
  smart-rf                 Smart-RF Management Commands
  spanning-tree            Display spanning tree information
  startup-config           Startup configuration
  terminal                 Display terminal configuration parameters
  timezone                 The timezone
  upgrade-status           Display last image upgrade status
  version                  Display software & hardware version
  wireless                 Wireless commands
rfs7000-37FABE(config)#
```

4.1.44 smart-rf-policy

Global Configuration Commands

Configures a Smart RF policy.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
smart-rf-policy <smart-rf-policy-name>
```

Parameters

<smart-rf-policy-name>	Enter the Smart RF policy name

Example

```
rfs7000-37FABE(config)#smart-rf-policy test
rfs7000-37FABE(config-smart-rf-policy-test)#
```

NOTE: For more information, see Chapter 21, SMART-RF-POLICY.

4.1.45 wips-policy

Global Configuration Commands

Configures a WIPS policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wips-policy <wips-policy-name>
```

Parameters

<wips-policy-name>	Enter the WIPS policy name to configure

Example

```
rfs7000-37FABE(config)#wips-policy test
rfs7000-37FABE(config-wips-policy-test)#
```

NOTE: For more information, see Chapter 22, WIPS-POLICY.

4.1.46 wlan

Global Configuration Commands

Configures a wireless LAN.

Table 4.16 *WLAN Commands*

Command	Description	Reference
wlan	Configures a wireless LAN.	*page 4-94*

4.1.46.1 wlan

wlan

Configures a WLAN.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wlan {[<WLAN>|containing <WORD>]}
```

Parameters

<WLAN>|containing <WORD>	Configures a wireless LAN • <WLAN> – Optional. Configures the WLAN specified by its WLAN number. • containing <WORD> – Optional. Specify WLANs that contain a sub-string in the WLAN name

Example

```
rfs7000-37FABE(config)#wlan 1
rfs7000-37FABE(config-wlan-1)#

rfs7000-37FABE(config)#wlan containing wlan1
rfs7000-37FABE(config-wlan-{'containing': 'wlan1'})#
```

4.1.46.2 wlan-mode commands

wlan

Configures WLAN related commands. Manual mapping of WLANs is erased when the actual WLAN is disabled and enabled immediately.

Use the (config) instance to configure WLAN related parameters.

To navigate to this instance, use the following commands:

```
rfs7000-37FABE(config)#wlan <WLAN>
```

Table 4.17 Summarizes wlan-mode commands

Table 4.17 *wlan-mode commands*

Command	Description	Reference
802.11k	Configures support for 802.11k radio resource measurement	*page 4-114*
802.11r	Configures support for 802.11r fast BSS transition	*page 4-115*
802.11w	Enables support for Protected Management Frame (IEEE 802.11w) settings	*page 4-116*
accounting	Defines the accounting configuration on this WLAN	*page 4-117*
acl	Defines the actions taken based on an ACL rule configuration	*page 4-118*
answer-broadcast-probes	Allows the WLAN to respond to probes for broadcast ESS	*page 4-119*
authentication-type	Sets the authentication type for the WLAN	*page 4-120*
bridging-mode	Configures how packets to/from this WLAN are bridged	*page 4-121*
broadcast-dhcp	Configures broadcast DHCP packet handling	*page 4-122*
broadcast-ssid	Advertises the SSID of the WLAN in beacons	*page 4-123*
captive-portal-enforcement	Configures the WLAN's captive-portal enforcement	*page 4-124*
client-access	Enables WLAN client-access (normal data operations) on the WLAN	*page 4-125*
client-client-communication	Allows the switching of frames from one wireless client to another on the WLAN	*page 4-126*
client-load-balancing	Enables load balancing of the clients on the specified WLAN	*page 4-127*
data-rates	Specifies the 802.11 rates to be supported on the WLAN	*page 4-128*

Table 4.17 *wlan-mode commands*

Command	Description	Reference
description	Sets the WLAN's description	*page 4-131*
encryption-type	Sets the encryption type for the WLAN	*page 4-132*
enforce-dhcp	Drops packets from clients with a static IP address	*page 4-133*
ip	Configures Internet Protocol (IP) settings	*page 4-134*
kerberos	Configures Kerberos authentication parameters	*page 4-135*
motorola-extensions	Enables support for Motorola Solutions-specific extensions to 802.11	*page 4-137*
no	Negates a command or sets its default value	*page 4-138*
proxy-arp-mode	Enables proxy-arp-mode for ARP requests	*page 4-139*
radius	Configures the RADIUS related parameters	*page 4-140*
shutdown	Closes the WLAN	*page 4-141*
ssid	Configures the SSID the WLAN	*page 4-142*
use	Defines WLAN mode configuration settings	*page 4-143*
vlan	Sets the VLAN assignment for the WLAN	*page 4-144*
vlan-pool-member	Adds a member VLAN to the pool of VLANs for the WLAN	*page 4-145*
wep128	Configures WEP128 parameters	*page 4-146*
wep64	Configures WEP64 parameters	*page 4-147*
wireless-client	Configures the transmit power for wireless clients transmission	*page 4-148*
wpa-wpa2	Modifies TKIP, CCMP (WPA/WPA2) related parameters	*page 4-150*

4.1.46.2.1802.11k

wlan-mode commands

Configures support for 802.11k radio resource measurement

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`802.11k {channel-report}`

Parameters

{channel-report}	Optional. Configures support for radio resource measurement, including the channel-report element in beacons and probe responses

Example

```
rfs7000-37FABE(config-wlan-1)#802.11k channel-report
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 802.11k channel-report
rfs7000-37FABE(config-wlan-1)#
```

4.1.46.2.2802.11r

wlan-mode commands

Configures support for 802.11r fast BSS transition

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`802.11r {mobility-domain-id <WORD>}`

Parameters

{mobility-domain-id} <WORD>	Configures the mobility domain ID for the roaming domain. A mobility domain ID must be 4 hexadecimal characters long.

Example

```
rfs7000-37AFBE(config-wlan-1)#802.11r mobility-domain-id 9f21
rfs7000-37AFBE(config-wlan-1)#
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 802.11r mobility-domain-id 9f21
```

4.1.46.2.3802.11w

wlan-mode commands

Enables support for Protected Management Frames (IEEE 802.11w) settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
802.11w [mandatory|optional|sa-query]
802.11w sa-query [attempts <1-15>|timeout <100-6000>]
```

Parameters

[mandatory|optional| sa-query]	• mandatory – Enforces protected management frame settings on the WLAN • optional – Advertises support for PMF but it is enforced only for clients that indicate their support • sa-query – Enables security association query settings • attempts <1-15> – Sets the number of times an sa-query message is attempted • timeout <100-6000> – Sets the timeout when waiting for a response to a security-association-query, before resending

Example

```
rfs7000-37FABE(config-wlan-wlan1)#802.11w sa-query timeout 110
rfs7000-37FABE(config-wlan-wlan1)#802.11w sa-query attempts 1
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 802.11r mobility-domain-id 9f21
 802.11w sa-query timeout 110
 802.11w sa-query attempts 1
```

4.1.46.2.4accounting

wlan-mode commands

Defines the WLAN's accounting configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
accounting [radius|syslog host <WORD> {port} <1-65535>]
```

Parameters

radius	Uses RADIUS accounting on this WLAN
syslog host <WORD> {port} <1-65535>	Uses syslog accounting on this WLAN • host – Enter a syslog destination hostname or IP address for accounting records • <WORD> – Enter the hostname or IP address • {port} <1-65535> – Enter a UDP port number for the syslog server from 1-65535

Example

```
rfs7000-37FABE(config-wlan-1)#accounting syslog host 172.16.10.12 port
rfs7000-37FABE(config-wlan-1)#accounting syslog host 172.16.10.12 port 2
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 accounting syslog host 172.16.10.12 port 2
```

4.1.46.2.5acl

wlan-mode commands

Defines the actions taken based on an ACL rule configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist
<0-86400>|disassociate}
```

Parameters

exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist <0-86400> |disassociate}	Sets the actions taken based on an ACL rule configuration
	• exceed-rate – Action is taken when the rate exceeds a set value
	• wireless-client-traffic <0-1000000> – The action is to deny traffic to the client
	  • <0-1000000> – Sets the packet data
	  • blacklist <0-86400> – Optional. Sets the time to blacklist a wireless client
	  • disassociate – When enabled, a client is disassociated

Example

```
rfs7000-37FABE(config-wlan-1)#acl exceed-rate wireless-client-denied-traffic 20
disassociate
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 acl exceed-rate wireless-client-denied-traffic 20 disassociate
```

4.1.46.2.6answer-broadcast-probes

wlan-mode commands

Allows the WLAN to respond to probe requests that do not specify an SSID to probe for broadcast ESS

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
answer-broadcast-probes
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#answer-broadcast-probes
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 answer-broadcast-probes
```

4.1.46.2.7 authentication-type

wlan-mode commands

Sets the authentication type for the WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]
```

Parameters

[eap|eap-mac|eap-psk| kerberos|mac|none]	Sets the authentication type for this WLAN • eap – EAP authentication (802.1X) • eap-mac – EAP or MAC authentication depending on client (valid only with no encryption or WEP) • eap-psk – EAP authentication or pre-shared-keys depending on client (valid only with TKIP/CCMP) • kerberos – Kerberos authentication (encryption will change to WEP128 if its not already WEP128/Keyguard) • mac – MAC authentication (RADIUS lookup of MAC address) • none – No authentication is used

Example

```
 authentication-type none
rfs7000-37FABE(config-wlan-1)#authentication-type eap
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type eap
 authentication-type none
```

4.1.46.2.8bridging-mode

wlan-mode commands

Configures how packets to/from this WLAN are bridged

Syntax

```
bridging-mode [local|tunnel]
```

Parameters

[local|tunnel]	• local – Packets are bridged between WLAN and local ethernet ports • tunnel – Packets are tunneled to other devices (typically wireless controllers)

Example

```
rfs7000-37FABE(config-wlan-1)#bridging-mode local
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode local
 encryption-type none
 authentication-type none
```

4.1.46.2.9broadcast-dhcp

wlan-mode commands

Configures broadcast DHCP packet handling

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
broadcast-dhcp validate-offer
```

Parameters

validate-offer	Validates the broadcast DHCP packets destined to a wireless client associated to the radio before forwarding them over the air

Example

```
rfs7000-37FABE(config-wlan-1)#broadcast-dhcp validate-offer
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 broadcast-dhcp validate-offer
```

4.1.46.2.10broadcast-ssid

wlan-mode commands

Advertises the WLAN SSID in beacons

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
broadcast-ssid
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#broadcast-ssid
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
```

4.1.46.2.11captive-portal-enforcement

wlan-mode commands

Configures the WLAN's captive-portal enforcement

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
captive-portal-enforcement {fall-back}
```

Parameters

{fall-back}	Enforces captive-portal validation if WLAN authentication fails (applicable to EAP or MAC)

Example

```
rfs7000-37FABE(config-wlan-1)#captive-portal-enforcement fall-back
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 captive-portal-enforcement fall-back
```

4.1.46.2.12client-access

wlan-mode commands

Enables WLAN client access (for normal data operations)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
client-access
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-wlan1)#client-access
```

4.1.46.2.13client-client-communication

wlan-mode commands

Allows switching of frames from one wireless client to another

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
client-client-communication
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-wlan1)#client-client-communication
```

4.1.46.2.14client-load-balancing

wlan-mode commands

Configures load balancing of wireless clients on the specified WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
client-load-balancing {allow-single-band-clients [2.4ghz|5ghz]|
band-discovery-intvl <0-10000> |capability-ageout-time <0-10000>|
max-probe-req|probe-req-intvl}
client-load-balancing {max-probe-req|probe-req-intvl} [2.4ghz|5ghz]
 <0-10000>
```

Parameters

{allow-single-band-clients [2.4ghz|5ghz]| band-discovery-intvl <0-10000> |capability-ageout-time <0-10000>| max-probe-req| probe-req-intvl}	• allow-single-band-clients [2.4ghz|5ghz] – Allows single band wireless clients to associate even during load balancing
	  • 2.4ghz – Enables balancing of loads across 2.4ghz channels
	  • 5ghz – Enables balancing of loads across 5ghz channels
	• band-discovery-intvl <0-10000> – Configures time interval to discover client's band capability before associating it
	• capability-ageout-time <0-10000> – Configures time before it ages out client's capability information
	• max-probe-req [2.4ghz|5ghz] <0-10000> – Configures client probe requests beyond which, it is allowed to associate
	• probe-req-intvl [2.4ghz|5ghz] <0-10000> – Configures interval for client probe requests beyond which, it is allowed to associate
	  • <0-1000> – Sets band discovery interval between 0 and 10000 seconds

Example

```
rfs7000-37FABE(config-wlan-wlan1)#client-load-balancing allow-single-band-clients
2.4ghz
rfs7000-37FABE(config-wlan-wlan1)#

rfs7000-37FABE(config-wlan-wlan1)#client-load-balancing band-discovery-intvl 2
rfs7000-37FABE(config-wlan-wlan1)#

rfs7000-37FABE(config-wlan-wlan1)#client-load-balancing probe-req-intvl 5ghz 5
rfs7000-37FABE(config-wlan-wlan1)#
```

4.1.46.2.15data-rates

wlan-mode commands

Specifies the 802.11 rates supported on the WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
data-rates [2.4GHz|5GHz]
data-rates 2.4GHz [b-only|bg|bgn|custom|default|g-only|gn]
data-rates 5GHz [a-only|an|custom|default]
data-rates 5GHz custom [{12|18|24|36|48|54|9|basic-1|basi-11|
basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|
basic-6|basic-9|basic-mcs0-7|mcs0-15|mcs0-7|mcs8-15}]
```

Parameters

2.4GHz [b-only|bg|bgn |custom|default|g-only|gn]	Specifies the 802.11 rates supported on the WLAN when mapped to a 2.4GHz radio • b-only – Supports 11b-only mode • bg – Uses rates that support both 11b and 11g clients • bgn – Uses rates that support 11b, 11g and 11n clients • custom – Configures a list of data rates by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it is to be used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11') • default – Uses the rates configured on the radio • g-only – Uses rates that support operation in 11g-only mode • gn – Uses rates that support 11g and 11n clients

5GHz [a-only|an| custom[{12|18|24|36|48|54|9 |basic-1|basi-11| basic-12|basic-18| basic-2|basic-24| basic-36|basic-48| basic-5.5|basic-54| basic-6|basic-9| basic-mcs0-7| mcs0-15|mcs0-7|mcs8-15}] |default]]	Specifies the 802.11 rates to be supported on the WLAN when mapped to a 5GHz radio • a-only – Uses rates that support operation in 11a-only mode • an – Uses rates that support 11a and 11n clients • default – Uses rates configured on the radio • custom [{12|18|24|36|48|54|9|basic-1|basi-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54| basic-6|basic-9|basic-mcs0-7|mcs0-15|mcs0-7|mcs8-15}] – Configures a list of data rates by specifying each rate individually. Using 'basic-' as prefix before a rate, indicates it is used as a basic rate (Eg: 'data-rates custom basic-1 basic-2 5.5 11')
{12|18|24|36|48|54|9|basic-1|basi-11| basic-12|basic-18| basic-2|basic-24| basic-36|basic-48| basic-5.5|basic-54| basic-6|basic-9| basic-mcs0-7| mcs0-15|mcs0-7|mcs8-15}] |default]	• 12 –12-Mbps • 18 – 18-Mbps • 24 – 24-Mbps • 36 – 36-Mbps • 48 – 48-Mbps • 54 – 54-Mbps • 6 – 6-Mbps • 9 – 9-Mbps • basic-1 – Basic 1-Mbps • basic-11– Basic 11-Mbps • basic-12 – Basic 12-Mbps • basic-18 – Basic 18-Mbps • basic-2 – Basic 2-Mbps • basic-24 – Basic 24-Mbps • basic-36 – Basic 36-Mbps • basic-48 – Basic 48-Mbps • basic-5.5 – Basic 5.5-Mbps • basic-54 – Basic 54-Mbps • basic-6 – Basic 6-Mbps • basic-9 – Basic 9-Mbps • basic-mcs0-7 – Modulation and coding scheme 0-7 as a basic rate • mcs0-15 – Modulation and coding scheme 0-15 • mcs0-7 – Modulation and coding scheme 0-7 • mcs8-15 – Modulation and coding scheme 8-15 • default – Uses rates configured on the radio]

Example

```
rfs7000-37FABE(config-wlan-1)#data-rates 2.4 gn
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 data-rates 2.4GHz gn
 authentication-type none
```

4.1.46.2.16description

wlan-mode commands

Defines the WLAN description. Used to identify the selected WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
description <LINE>
```

Parameters

<LINE>	Defines the description for this WLAN. It is used to identify the selected WLAN.

Example

```
rfs7000-37FABE(config-wlan-1)#description testwlan
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 description testwlan
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
```

4.1.46.2.17encryption-type

wlan-mode commands

Sets the WLAN encryption type

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
encryption-type [ccmp|keyguard|none|tkip|tkip-ccmp|wep128|
web128-keyguard]
```

Parameters

[ccmp|keyguard|none|tkip|tkip-ccmp|wep128| web128-keyguard]	Sets the WLAN encryption type. Options include: • ccmp – AES Counter Mode CBC-MAC Protocol (AES-CCM CCMP) • keyguard – Keyguard-MCM (Mobile Computing Mode) • none – No encryption • tkip – Enables Temporal Key Integrity Protocol (TKIP) • tkip-ccmp – Enables both TKIP and CCMP on this WLAN • wep128 – Enables Wired Equivalence Privacy (WEP) with 128 bit keys • wep128-keyguard – Enables WEP128 as well as Keyguard-MCM on this WLAN

Example

```
#

rfs7000-37FABE(config-wlan-1)#encryption-type tkip-ccmp
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type tkip-ccmp
 authentication-type none
```

4.1.46.2.18enforce-dhcp

wlan-mode commands

Drops the packets from clients with a static IP address.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
enforce-dhcp
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#enforce-dhcp
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 enforce-dhcp
```

4.1.46.2.19ip

wlan-mode commands

Configures Internet Protocol settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip [arp|dhcp]
ip dhcp trust
ip arp [header-mismatch-validation|trust]
```

Parameters

[arp|dhcp] trust	Sets Internet Protocol settings for ARP and DHCP packets.
	• arp [header-mismatch-validation|trust] – Address Resolution Protocol configuration
	  • header-mismatch-validation– Verifies mismatch for source MAC in ARP header and ethernet header
	• dhcp trust – Dynamic Host Resolution Protocol configuration
	  • trust – Sets the ARP/DHCP responses as trusted for this WLAN/ range

Example

```
rfs7000-37FABE(config-wlan-1)#ip dhcp trust
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 ip dhcp trust
```

4.1.46.2.20kerberos

wlan-mode commands

Configures Kerberos authentication parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
kerberos [password|realm <WORD>|server]
kerberos password [0 <LINE>|2 <LINE>|<LINE>]
kerberos server [primary|secondary|timeout]
kerberos server primary host <IP> {port} <1-65535>
kerberos server secondary host <IP> {port} <1-65535>
kerberos server timeout <1-60>
```

Parameters

[password|realm|server	• password [0|2|<LINE>] – Creates a KDC server password (up to 127 characters)
	  • 0 <LINE> – Enter the password
	  • 2 <LINE> – Enter the password in encrypted form
	  • <LINE> – The password
	• realm <WORD> – Defines a KDC realm (up to 127 characters)
	• server [primary|secondary|timeout] – Modifies KDC server parameters
	  • primary host <IP> {port <1-65535>} – Defines the primary KDC server
	  • secondary host <IP> {port <1-65535>} – Defines the secondary KDC server
	  • host – Enter the address of the KDC server
	  • <IP> {port <1-65535>} – Sets the KDC server IP address
	  • port <1-65535> – Optional. Sets the KDC server authentication port in the range 1 to 65535. The default value is 88
	  • timeout <1-60> – Modifies the KDC server's timeout parameters
	  • <1-60> – Defines the time the controller waits for a response from the KDC server before retrying

Example

```
rfs7000-37FABE(config-wlan-1)#kerberos server timeout 12
rfs7000-37FABE(config-wlan-1)#

rfs7000-37FABE(config-wlan-1)#kerberos server primary host 172.16.10.9 port 88
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 kerberos server timeout 12
 kerberos server primary host 172.16.10.9
```

4.1.46.2.21motorola-extensions

wlan-mode commands

Enables support for Motorola Solutions-specific extensions to 802.11

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
motorola-extensions [move-command|smart-scan|symbol-load-information|
wmm-load-information]
```

Parameters

[move-command| smart-scan| symbol-load-information| wmm-load-information]	• move-command – Enables support for Motorola-move (fast roaming) • smart-scan – Enables support for smart scanning • symbol-load-information – Enables support for the Symbol Technologies load information element (Element ID 173) • wmm-load-information – Enables support for the Motorola Solutions WMM load information element

Example

```
rfs7000-37FABE(config-wlan-1)#motorola-extensions wmm-load-information
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 motorola-extensions wmm-load-information
```

4.1.46.2.22no

wlan-mode commands

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no <parameter>
```

Parameters

None

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-wlan-wlan1)#no wep64 key 1
rfs7000-37FABE(config-wlan-wlan1)#

rfs7000-37FABE(config-wlan-wlan1)#no ip arp trust
rfs7000-37FABE(config-wlan-wlan1)#
```

4.1.46.2.23proxy-arp-mode

wlan-mode commands

Enables proxy-arp mode for handling ARP requests

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
proxy-arp-mode [dynamic|strict]
```

Parameters

[dynamic|strict]	• dynamic – Forwards ARP requests to the wireless side (for which a response could not be proxied) • strict – Does not forward ARP requests to the wireless side

Example

```
rfs7000-37FABE(config-wlan-1)#proxy-arp-mode strict
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 proxy-arp-mode strict
```

4.1.46.2.24radius

wlan-mode commands

Configures RADIUS related parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
radius [dynamic-authorization|nas-identifier <WORD>|nas-port-id <WORD>|vlan-assignment]
```

Parameters

dynamic-authorization	Enables support for disconnect and change-of-authorization messages (RFC5176)
nas-identifier <WORD>	The WLAN NAS identifier sent to the RADIUS server. Maximum length is 256 characters
nas-port-id <port>	The WLAN NAS-port-id sent to the RADIUS server. Maximum length is 256 characters
vlan-assignment	Sets the VLAN assignment of this WLAN

Example

```
rfs7000-37FABE(config-wlan-1)#radius vlan-assignment
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid WLAN_USECASE_01
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 radius vlan-assignment
```

4.1.46.2.25shutdown

wlan-mode commands

Closes the WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
shutdown
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-1)#shutdown
```

4.1.46.2.26ssid

wlan-mode commands

Configures the SSID for the WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ssid <WORD>
```

Parameters

<WORD>	Enter the SSID of this WLAN <ssid> up to 32 characters

Example

```
rfs7000-37FABE(config-wlan-1)#ssid Test1
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid Test1
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
```

4.1.46.2.27use

wlan-mode commands

Sets setting to use the aaa policy configured for the WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
use [aaa-policy <aaa-policy-name>|association-acl-policy <association-policy-
name>|captive-portal <captive-portal-name>|ip-access-list <ip-access-list-name>|mac-
access-list <mac-access-list-name>|wlan-qos-policy <wlan-qos-policy-name>]

use ip-access-list [in|out] <ip-access-list-name>
use mac-access-list [in|out] <mac-access-list-name>
```

Parameters

aaa-policy <aaa-policy-name>	Uses the aaa policy for the WLAN • <aaa-policy-name> – Enter the aaa-policy to use
association-acl <association-policy-name>	Uses the association-acl policy for the WLAN • <association-policy-name> – Enter the association-policy to use
captive-portal <captive-portal-name>	Enables the WLAN's captive-portal authentication
ip-access-list [in|out] <ip-access-list-name>	Specifies the ip-access-list used • in – Incoming packets • out – Outgoing packets • <ip-access-list-name> – Enter the ip-access-list to use
mac-access-list [in|out] <mac-access-list-name>	Specifies the mac-access-list used • in – Incoming packets • out – Outgoing packets • <ip-access-list-name> – Enter the mac-access-list to use
wlan-qos-policy <wlan-qos-policy-name>	Uses the wlan-qos-policy for the WLAN • <wlan-qos-policy-name> – Enter the wlan-qos-policy to use

Example

```
rfs7000-37FABE(config-wlan-1)#use ip-access-list in symbol
rfs7000-37FABE(config-wlan-1)#
```

4.1.46.2.28vlan

wlan-mode commands

Sets the VLAN assignment of the WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
vlan <1-4094>
```

Parameters

<1-4094>	Sets the WLAN's VLAN. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased.

Example

```
rfs7000-37FABE(config-wlan-wlan1)#vlan 4
rfs7000-37FABE(config-wlan-wlan1)#

rfs7000-37FABE(config-wlan-wlan1)#show interface vlan 4
Interface vlan4 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 5, Metric: 1, MTU: 1500
  IP-Address: 157.235.208.252/24
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

rfs7000-37FABE(config-wlan-wlan1)#
```

4.1.46.2.29vlan-pool-member

wlan-mode commands

Add a member vlan to the pool of VLANs for the WLAN

NOTE: Configuration of a VLAN pool overrides the 'vlan' configuration.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xxx
- AP650
- AP6511
- AP6532

Syntax

```
vlan-pool-member <WORD> {limit} <0-8192>
```

Parameters

<WORD> {limit} <0-8192>	Defines the VLAN configuration. It can be either a single index, or a list (1,3,7) • limit <0 -8192> – Optional. It can be ignored if the number of clients are limited and expected to be well within the limits of the DHCP pool on the vlan. • <0-8192> – Specifies the number of users allowed

Example

```
rfs7000-37FABE(config-wlan-1)#vlan-pool-member 1-10 limit 1
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid Test1
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 vlan-pool-member 1 limit 1
 vlan-pool-member 2 limit 1
 vlan-pool-member 3 limit 1
 vlan-pool-member 4 limit 1
 vlan-pool-member 5 limit 1
 vlan-pool-member 6 limit 1
 vlan-pool-member 7 limit 1
 vlan-pool-member 8 limit 1
 vlan-pool-member 9 limit 1
 vlan-pool-member 10 limit 1
 vlan-pool-member 11 limit 1
 vlan-pool-member 12 limit 1
 vlan-pool-member 13 limit 1
 vlan-pool-member 14 limit 1
 vlan-pool-member 15 limit 1
 vlan-pool-member 16 limit 1
```

4.1.46.2.30wep128

wlan-mode commands

Configures WEP128 parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wep128 [key|keys-from-passkey|transmit-key]
wep128 key <1-4> [ascii|hex] [0|2|<WORD>]
wep128 keys-from-passkey <WORD>
wep128 transmit-key <1-4>
```

Parameters

key <1-4> [ascii|hex] [0|2|<WORD>]	key <1-4> [ascii|hex] – Configures pre-shared hex keys
	• ascii [0|2|<WORD>] – Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128)
	  • <WORD> – Keys as 13 ascii characters that are converted to hex, or 26 hexadecimal characters or as a 64 characters hexadecimal value if encrypted
	• hex [0|2|<WORD>] – Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128)
	  • 0 – Enter a clear text key
	  • 2 – Enter an encrypted key
	  • <WORD> – Keys as 13 ascii characters that are converted to hex, or 26 hexadecimal characters

keys-from-passkey <WORD>	Specifies a passphrase from which keys are derived • <WORD> – Sets the passphrase (between 4 and 32 characters)
transmit-key <1-4>	Defines the key index used for transmission from an AP to a client

Example

```
rfs7000-37FABE(config-wlan-1)#wep128 transmit-key 1
rfs7000-37FABE(config-wlan-1)#
```

4.1.46.2.31wep64

wlan-mode commands

Configures WEP64 parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wep64 [key|keys-from-passkey|transmit-key]
wep64 key <1-4> [ascii|hex] [0|2|<WORD>]
wep64 keys-from-passkey <WORD>
wep64 transmit-key <1-4>]
```

Parameters

key <1-4> [ascii|hex] [0|2|<WORD>]	key <1-4> [ascii|hex] – Configures pre-shared hex keys
	• ascii [0|2|<WORD>] – Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128)
	• hex [0|2|<WORD>] – Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128)
	  • 0 – Enter a clear text key
	  • 2 – Enter an encrypted key
	  • <WORD> – Key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128)

keys-from-passkey <WORD>	Specifies a passphrase from which keys are derived • <WORD> – Sets the passphrase (between 4 and 32 characters)
transmit-key <1-4>	Defines the key index used for transmission from an AP to client

Example

```
rfs7000-37FABE(config-wlan-1)#wep64 key 1 ascii symbo
rfs7000-37FABE(config-wlan-1)#

rfs7000-37FABE(config-wlan-1)#wep64 transmit-key 1
rfs7000-37FABE(config-wlan-1)#
```

4.1.46.2.32wireless-client

wlan-mode commands

Configures the transmit power indicated to wireless clients for transmission

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wireless-client [cred-cache-ageout <60-86400>|hold-time <1-300>
|inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>|
reauthentication <30-86400>|tx-power <0-20>|vlan-cache-out <60-86400>]
```

Parameters

cred-cache-ageout <60-86400>|hold-time <1-300> |inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>| reauthentication <30-86400>|tx-power <0-20>|vlan-cache-out <60-86400>	• cred-cache-ageout <60-86400> – Configures the timeout for which the client credentials such as encryption keys are cached across associations
	  • <60-86400> – Specify the timeout between 60 and 86400 seconds
	• hold-time <1-300> – Time for which wireless client state information is cached post roaming
	  • <1-300> – Specify the hold time between 1 and 300 seconds
	• inactivity-timeout <60-86400> – Specifies an inactivity timeout in seconds. If a frame is not received from a wireless client for this amount of time, the client is disassociated
	• max-firewall-sessions <10-10000> – Specifies the maximum firewall sessions allowed per wireless client on the wlan
	  • <10-10000> – Specify the maximum number of firewall sessions allowed between 10 and 10000
	• reauthentication <30-86400> – Configures periodic reauthentication of associated clients
	  • <30-86400> – Sets the reauthentication time period between 30 and 86400 seconds
	• tx-power <0-20> – Configures the transmit power indicated to wireless clients for transmission
	  • <0-20> – Sets the transmit power in dBm
	• vlan-cache-ageout <60-86400> – Configures the timeout for which client VLAN information is cached across associations
	  • <60-86400> – Sets the timeout between 60 and 86400 seconds

Example

```
rfs7000-37FABE(config-wlan-1)#wireless-client cred-cache-ageout 65
rfs7000-37FABE(config-wlan-1)#wireless-client hold-time 10
rfs7000-37FABE(config-wlan-1)#wireless-client max-firewall-sessions 100
rfs7000-37FABE(config-wlan-1)#wireless-client reauthentication 35
rfs7000-37FABE(config-wlan-1)#wireless-client tx-power 12
```

```
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid Test1
 vlan 2
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 wireless-client cred-cache-ageout 65
 wireless-client hold-time 10
 wireless-client max-firewall-sessions 100
 wireless-client reauthentication 35
 wireless-client tx-power 12
```

4.1.46.2.33wpa-wpa2

wlan-mode commands

Modifies TKIP-CCMP (WPA/WPA2) related parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wpa-wpa2 [exclude-wpa2-tkip|handshake|key-rotation|opp-pmk-caching|
pmk-caching|preauthentication|psk|tkip-countermeasures]
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority
[high_|normal||timeout <10-5000>]
wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>
wpa-wpa2 psk [0|2|<LINE>] <LINE>
wpa-wpa2 tkip-countermeasures holdtime <0-65535>]
```

Parameters

exclude-wpa2-tkip	Excludes the WPA2 version of TKIP, support only WPA-TKIP
handshake [attempts <1-5>|init-wait <5-1000000>| priority|timeout <10-5000>]	Configures the parameters related to the WPA/WPA2 handshake • attempts <1-5> – Configures the total number of times a message is transmitted towards a non-responsive client • init-wait <5-1000000> – Configure a wait-time before the first message of the handshake is transmitted from the AP • priority [high|normal] – Configure the relative priority of the handshake messages compared to other data traffic • high – Treats handshake messages as high priority packets in the radio • normal – Treats handshake messages as normal priority packets in the radio • timeout <10-5000> – Configures the timeout for a handshake message, before it is retried
key-rotation [broadcast|unicast] <30-86400>	Configures parameters related to periodic rotation of encryption keys • broadcast – Sets the rotation of keys used for broadcast and multicast traffic • unicast – Sets the rotation of keys used for unicast traffic • <30-86400> – Specify the time in seconds when the keys are rotated
opp-pmk-caching	Enables the use of opportunistic key caching (same PMK across APs for fast roaming with EAP.802.1x)
pmk-caching	Enables the use of cached pairwise master keys (fast roaming with eap/802.1x)
preauthentication	Enables preauthentication usage (WPA2 fast roaming)
psk[0|2|<LINE>] <LINE>	• psk – Configures a pre-shared key The following parameters are common for the above: • 0 – Enter a clear text key • 2 – Enter an encrypted key • <LINE> – Enter pre-shared key either as a passphrase between 8 and 63 characters long, or as a 64 character (256bit) hexadecimal value • <LINE> – Enter pre-shared key either as a passphrase between 8 and 63 characters long, or as a 64 character (256bit) hexadecimal value
tkip-countermeasures holdtime <0-65535>	Configures TKIP countermeasures related parameters • <holdtime <0-65535> – Configures the amount of time a WLAN is disabled when TKIP counter measures are invoked • <0-65535> – Enter the hold-time in seconds

Example

```
rfs7000-37FABE(config-wlan-wlan1)#wpa-wpa2 tkip-countermeasures hold-time 2
rfs7000-37FABE(config-wlan-1)#show context
wlan 1
 ssid Test1
 vlan 2
 bridging-mode tunnel
```

```
encryption-type none
authentication-type none
wpa-wpa2 tkip-countermeasures hold-time 1000
```

4.1.47 wlan-qos-policy

Global Configuration Commands

Configures a WLAN QoS policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wlan-qos-policy <wlan-qos-policy-name>
```

Parameters

<wlan-qos-policy-name>	Enter a WLAN QoS-policy name to configure

Example

```
rfs7000-37FABE(config)#wlan-qos-policy test
rfs7000-37FABE(config-wlan-qos-test)#
```

NOTE: For more information, see Chapter 23, WLAN-QOS-POLICY.

4.1.48 write

Global Configuration Commands

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
write [terminal|memory]
```

Parameters

memory	Writes to the NV memory
terminal	Writes to terminal

Example

```
rfs7000-37FABE#write memory
[OK]
rfs7000-37FABE#


rfs7000-37FABE#write terminal
!
! Configuration of RFS7000 version 5.1.0.0-061D
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 enable
 calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
 voice-prioritization
 svp-prioritization
 wmm background cw-max 8
 wmm video txop-limit 9
.....................................................................rfs7000-
37FABE>
```

CHAPTER 5 COMMON COMMANDS

This chapter describes the CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes.

The PRIV EXEC command set contains commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either the USER EXEC mode or the PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

5.1 Common Commands

Table 5.1 Summarizes Common Commands

Table 5.1 *Common Commands in Controller*

Command	Description	Reference
clrscr	Clears the display screen	*page 5-3*
commit	Commits all changes made in the active session	*page 5-4*
exit	Ends the current mode and moves to the previous mode	*page 5-5*
help	Displays the interactive help system	*page 5-6*
no	Negates a command or sets its defaults	*page 5-10*
show	Shows running system information	*page 5-12*
revert	Reverts the changes made to their last saved configuration	*page 5-14*
service	Services or debugs the controller	*page 5-15*
write	Writes the system running configuration to memory or terminal	*page 5-35*

5.1.1 clrscr

Common Commands

Clears the screen and refreshes the prompt (**#**)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clrscr
```

Parameters

None

Example

```
rfs7000-37FABE>clrscr
rfs7000-37FABE>
```

5.1.2 commit

Common Commands

Commits all changes made in the active session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`commit {write}{memory}`

Parameters

write	If a commit succeeds, the configuration is written to memory
memory	Writes to memory

Example

```
rfs7000-37FABE>commit write memory
[OK]
rfs7000-37FABE>
```

5.1.3 exit

Common Commands

Ends the current mode and moves to the previous mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE(config)#exit
rfs7000-37FABE#
```

5.1.4 help

Common Commands

Describes the interactive help system

Use this command to access the advanced help feature. Use "**?**" anytime at the command prompt to access the help topic

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
help {show configuration-tree|search}
help search <WORD> {detailed|only-show|skip-show|skip-no}
```

Parameters

show configuration-tree	Displays running system information • configuration-tree – Displays the relationships amongst configuration objects
search <WORD> {detailed|only-show|skip-show|skip-no}	Searches for CLI commands related to a specific term • <WORD> – Enter a target term for a search (Eg: a feature or a configuration parameter) • detailed – Searches and displays help strings in addition to mode and commands • only-show – Displays only "show" commands, not configuration commands • skip-show – Displays only configuration commands, not "show" commands • skip-no – Displays only configuration commands, not 'no' commands

Example

```
rfs7000-37FABE>help search crypto detailed
Found 29 references for "crypto"
      Found 113 references for "crypto"

Mode    : User Exec
Command : show crypto key rsa (|public-key-detail) (|(on DEVICE-NAME))
           \ Show running system information
            \ Encryption related commands
             \ Key management operations
              \ Show RSA public Keys
               \ Show the public key in PEM format
                \ On AP/Controller
                 \ AP / Controller name

        : show crypto pki trustpoints (WORD|all|)(|(on DEVICE-NAME))
                  \ Show running system information
                  \ Encryption related commands
                  \ Public Key Infrastructure related commands
                  \ Display the configured trustpoints
                  \ Display a particular trustpoint's details
                  \ Display details for all trustpoints
                  \ On AP/Controller
                   \ AP / Controller name

        : show crypto isakmp sa (|(on DEVICE-NAME))
                   \ Show running system information
                   \ Encryption Module
                   \ Show ISAKMP related statistics
                   \ Show all ISAKMP Security Associations
                   \ On AP/Controller
                   \ AP / Controller name

        : show crypto ipsec sa (|(on DEVICE-NAME))
                   \ Show running system information
                   \ Encryption Module
                   \ Show IPSec related statistics
                   \ IPSec security association
                   \ On AP/Controller
                   \ AP / Controller name

        : crypto key generate rsa WORD <1024-2048> (|(on DEVICE-NAME))
                   \ Encryption related commands
                   \ Key management operations
                   \ Generate a keypair
                   \ Generate a RSA keypair
                   \ Keypair name
................................................................................
.............................................................rfs7000-37FABE>

rfs7000-37FABE>help show configuration-tree

 ## ACCESS-POINT / SWITCH ## ---+
                               |
                               +--> [[ RF-DOMAIN ]]
                               |
                               +--> [[ PROFILE ]]
                               |
                             +--> Device specific parameters (license, serial number,
hostname)
                               |
                              +--> Configuration Overrides of rf-domain and profile

 ## RF-DOMAIN ## ---+
                    |
                    +--> RF parameters, WIPS server parameters
                    |
                    +--> [[ SMART-RF-POLICY ]]
                    |
```

```
                    +--> [[ WIPS POLICY ]]

 ## PROFILE ## ---+
                  |
                  +--> Physical interface (interface GE,ME,UP etc)
                  |                          |
                  |                          +--> [[ RATE-LIMIT-TRUST-POLICY ]]
                  |
                  +--> Vlan interface (interface VLAN1/VLAN36 etc)
                  |
                  +--> Radio interface (interface RADIO1, RADIO2 etc)
                  |                            |
                  |                            +--> Radio specific Configuration
                  |                            |
                  |                            +--> [[ RADIO-QOS-POLICY ]]
                  |                            |
                  |                            +--> [[ ASSOC-ACL-POLICY ]]
                  |                            |
                  |                            +--> [[ WLAN ]]
                  |
                  +--> [[ MANAGEMENT-POLICY ]]
                  |
                  +--> [[ DHCP-SERVER-POLICY ]]
                  |
                  +--> [[ FIREWALL-POLICY ]]
                  |
                  +--> [[ NAT-POLICY ]]
.....................................................................................
.....................................................rfs7000-37FABE>

rfs7000-37FABE>help search clrscr only-show
found no commands containing "clrscr"
rfs7000-37FABE>


rfs7000-37FABE>help search service skip-show
Found 32 references for "service"

Mode    : User Exec
Command : service show cli
        : service show rim config (|include-factory)
        : service show wireless credential-cache
        : service show wireless neighbors
        : service show general stats(|(on DEVICE-OR-DOMAIN-NAME))
        : service show process(|(on DEVICE-OR-DOMAIN-NAME))
        : service show mem(|(on DEVICE-OR-DOMAIN-NAME))
        : service show top(|(on DEVICE-OR-DOMAIN-NAME))
        : service show crash-info (|(on DEVICE-OR-DOMAIN-NAME))
        : service cli-tables-skin
(none|minimal|thin|thick|stars|hashes|percent|ansi|utf-8) (grid|)
        : service cli-tables-expand (|left|right)
        : service wireless clear unauthorized aps (|(on DEVICE-OR-DOMAIN-NAME))
        : service wireless qos delete-tspec AA-BB-CC-DD-EE-FF tid <0-7>
        : service wireless wips clear-event-history
        : service wireless wips clear-mu-blacklist (all|(mac AA-BB-CC-DD-EE-FF))
        : service radio <1-3> dfs simulate-radar (primary|extension)
        : service smart-rf run-calibration
        : service smart-rf stop-calibration
        : service cluster manual-revert
        : service advanced-wips clear-event-history
        : service advanced-wips clear-event-history (dos-eap-failure-spoof|id-theft-
out-of-sequence|id-theft-eapol-success-spoof-detected|wlan-jack-attack-
detected|essid-jack-attack-detected|monkey-jack-attack-detected|null-probe-response-
detected|fata-jack-detected|fake-dhcp-server-detected|crackable-wep-iv-used|windows-
zero-config-memory-leak|multicast-all-systems-on-subnet|multicast-all-routers-on-
subnet|multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-
detection|multicast-rip2-routers-detection|multicast-igmp-routers-
detection|multicast-vrrp-agent|multicast-hsrp-agent|multicast-dhcp-server-relay-
agent|multicast-igmp-detection|netbios-detection|stp-detection|ipx-
detection|invalid-management-frame|invalid-channel-advertized|dos-deauthentication-
```

```
detection|dos-disassociation-detection|dos-rts-flood|rogue-ap-detection|accidental-
association|probe-response-flood|dos-cts-flood|dos-eapol-logoff-storm|unauthorized-
bridge)
        : service start-shell
        : service pktcap on(bridge|drop|deny|router|wireless|vpn|radio (all|<1-3>)
(|promiscuous)|rim|interface `WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>')(|{direction
(any|inbound|outbound)|acl-name WORD|verbose|hex|count <1-1000000>|snap <1-
2048>|write (FILE|URL|tzsp WORD)|tcpdump})(|filter LINE)

Mode    : Profile Mode
Command : service watchdog

Mode    : Radio Mode
Command : service antenna-type (default|dual-
band|omni|yagi|embedded|panel|patch|sector|out-omni|in-patch|AP650-int)
        : service disable-erp
        : service disable-ht-protection
        : service recalibration-interval <0-65535>
.....................................................................rfs7000-
37FABE>

rfs7000-37FABE>help search mint only-show
Found 8 references for "mint"

Mode    : User Exec
Command : show mint neighbors (|details)(|(on DEVICE-NAME))
        : show mint links (|details)(|(on DEVICE-NAME))
        : show mint id(|(on DEVICE-NAME))
        : show mint stats(|(on DEVICE-NAME))
        : show mint route(|(on DEVICE-NAME))
        : show mint lsp
        : show mint lsp-db (|details)(|(on DEVICE-NAME))
        : show mint mlcp(|(on DEVICE-NAME))
rfs7000-37FABE>
```

5.1.5 no

Common Commands

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no <parameter>
```

Parameters

None

Example

```
rfs7000-37FABE#no ?
  adoption         Reset adoption state of the device (& all devices adopted to
                   it)
  captive-portal   Captive portal commands
  crypto           Encryption related commands
  debug            Debugging functions
  logging          Modify message logging facilities
  page             Toggle paging
  service          Service Commands
  terminal         Set terminal line parameters
  upgrade          Remove a patch
  wireless         Wireless Configuration/Statistics commands
rfs7000-37FABE#no

 rfs7000-37FABE(config)#no ?
  aaa-policy                Delete a aaa policy
  adoption-policy           Delete an adoption policy
  advanced-wips-policy      Delete an advanced-wips policy
  ap650                     Delete an AP650 access point
  ap6511                    Delete an AP6511 access point
  ap6532                    Delete an AP6532 access point
  ap7131                    Delete an AP7131 access point
  association-acl-policy    Delete an association-acl policy
  captive-portal            Delete a captive portal
  critical-resource-policy  Remove device onboard critical resource policy
  customize                 Restore the custom cli commands to default
  device                    Delete mulitple devices
  device-categorization     Delete  device categorization object
  dhcp-server-policy        DHCP server policy
  dns-whitelist             Delete a whitelist object
  event-system-policy       Delete a event system policy
  firewall-policy           Configure firewall policy
  igmp-snoop-policy         Remove device onboard igmp snoop policy
  ip                        Internet Protocol (IP)
  mac                       MAC configuration
  management-policy         Delete a management policy
  nac-list                  Delete an network access control list
  password-encryption       Disable password encryption in configuration
  profile                   Delete a profile and all its associated
                            configuration
  radio-qos-policy          Delete a radio QoS configuration policy
```

```
  radius-group                Local radius server group configuration
  radius-server-policy        Remove device onboard radius policy
  radius-user-pool-policy     Configure Radius User Pool
  rf-domain                   Delete one or more RF-domains and all their
                              associated configurations
  rfs4000                     Delete an RFS4000 wireless controller
  rfs6000                     Delete an RFS6000 wireless controller
  rfs7000                     Delete an RFS7000 wireless controller
  role-policy                 Role based firewall policy
  smart-rf-policy             Delete a smart-rf-policy
  wips-policy                 Delete a wips policy
  wlan                        Delete a wlan object
  wlan-qos-policy             Delete a wireless lan QoS configuration policy

  service                     Service Commands
rfs7000-37FABE(config)#
```

5.1.6 show

Common Commands

Displays running system information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show <parameter>
```

Parameters

None

Example

```
rfs7000-37FABE>show ?
    adoption             Display information related to adoption to wireless
                        controller
  advanced-wips           Advanced WIPS
  ap-upgrade              AP Upgrade
  boot                    Display boot configuration.
  captive-portal          Captive portal commands
  cdp                     Cisco Discovery Protocol
  clock                   Display system clock
  cluster                 Cluster Protocol
  commands                Show command lists
  context                 Information about current context
  critical-resources      Critical Resources
  crypto                  Encryption related commands
  debug                   Debugging functions
  debugging               Debugging functions
  device-categorization   Device Categorization
  event-history           Display event history
  event-system-policy     Display event system policy
  file                    Display filesystem information
  firewall                Wireless Firewall
  interface               Interface Configuration/Statistics commands
  ip                      Internet Protocol (IP)
  ip-access-list-stats    IP Access list stats
  licenses                Show installed licenses and usage
  lldp                    Link Layer Discovery Protocol
  mac-access-list-stats   MAC Access list stats
  mac-address-table       Display MAC address table
  mint                    MiNT protocol
  noc                     Noc-level information
  ntp                     Network time protocol
  password-encryption     Pasword encryption
  power                   Show power over ethernet command
  remote-debug            Show details of remote debug sessions
  rf-domain-manager       Show RF Domain Manager selection details
  role                    Role based firewall
  running-config          Current operating configuration
  session-changes         Configuration changes made in this session
  session-config          This session configuration
  sessions                Display CLI sessions
  smart-rf                Smart-RF Management Commands
```

```
  spanning-tree          Display spanning tree information
  startup-config         Startup configuration
  terminal               Display terminal configuration parameters
  timezone               The timezone
  upgrade-status         Display last image upgrade status
  version                Display software & hardware version
  wireless               Wireless commands

rfs7000-37FABE>
```

5.1.7 revert

Common Commands

Reverts any changes made to their last saved configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
revert
```

Parameters

None

Example

```
rfs7000-37FABE>revert
rfs7000-37FABE>
```

5.1.8 service

Common Commands

Service commands are used to manage the Controller configuration in all modes. Depending on the mode, different service commands display

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax User Exec Mode

```
service [advanced-wips|clear|cli-tables-expand|cli-tables-skin|cluster
|locator|noc|pktcap|radio|set|show|smart-rf|wireless]

service advanced-wips [clear-event-history|terminate-device]
service advanced-wips clear-event-history {accidental-association||
crackable-wep-iv-used|dos-cts-flood|dos-deauthentication-detection|
dos-disassociation-detection|dos-eap-failure-spoof|
dos-eapol-logoff-storm|dos-rts-flood|essid-jack-attack-detected|
fake-dhcp-server-detected|fata-jack-detected|
id-theft-eapol-success-spoof-detected|
id-theft-out-of-sequence|invalid-channel-advertized|
invalid-management-frame|ipx-detection|
monkey-jack-attack-detected|multicast-all-routers-on-subnet|
multicast-all-systems-on-subnet|
multicast-dhcp-server-relay-agent|
multicast-hsrp-agent|multicast-igmp-detection|
multicast-igrp-routers-detection|
multicast-ospf-all-routers-detection|
multicast-ospf-designated-routers-detection|
multicast-rip2-routers-detection|
multicast-vrrp-agent|netbios-detection|
null-probe-response-detected|probe-response-flood|rogue-ap-detection|
stp-detection|unathorized-bridge|windows-zero-config-memory-leak|
wlan-jack-attack-detected}
service advanced-wips terminate-device <MAC>

service clear [ap-upgrade history|command-history|noc|reboot-
history|unsanctioned|upgrade-history|wireless]
service clear [command-history|reboot-history|
upgrade-history]{on <DEVICE-NAME>}
service clear noc statistics
service clear  unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}]
service clear wireless [ap|client|radio|wlan]

service clear wireless ap statistics {<MAC>|on}
service clear wireless ap statistics <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless ap statistics {on <DEVICE-OR-DOMAIN-NAME>}

service clear wireless client statistics {<MAC>|on}
service clear wireless client statistics <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless client statistics {on <DEVICE-OR-DOMAIN-NAME>}

service clear wireless radio statistics {<DEVICE-NAME>|on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless radio statistics <DEVICE-NAME> {<1-3>|on}
service clear wireless radio statistics <DEVICE-NAME> <1-3> {on <DEVICE-OR-DOMAIN-
NAME>}
```

```
service clear wireless radio statistics <DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}

service clear wireless wlan statistics {<WLAN>|on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless wlan statistics <WLAN> {on <DEVICE-OR-DOMAIN-NAME>}

service cli-tables-expand {left|right}
service cli-tables-skin [ansi|hashes|minimal|none|percent|
stars|thick|thin|uf-8] {grid}
service cluster manual-revert
service locator {on <DEVICE-NAME>}
service noc parallel-updates <1-1024>

service pktcap on [bridge|deny|drop|ext-vlan|interface|radio|rim|router|
vpn|wireless] {acl-name <WORD>|count <1-1000000>|
direction[any|inbound|outbound]|filter <LINE>|hex|rate <1-100>|snap <1-
2048>|tcpdump|verbose|write [file|url|tzsp]}
service pktcap on interface [<WORD>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>]
service pktcap on radio [<1-3>|all]{acl-name <WORD>|count <1-1000000> |direction
[any|inbound|outbound]|filter <LINE>|hex|promiscuous|rate <1-100>|snap <1-
2048>|tcpdump|verbose|write [file|url|tzsp]}

service radio <1-3> [data-rates|dfs]
service radio <1-3> data-rates rate-index <0-27> [basic|supp]
service radio <1-3> dfs simulate-radar [extension|primary]

service set validation-mode [full|partial]{on <DEVICE-NAME>}

service show [advanced-wips|captive-portal|cli|command-history|
crash-info|dhcp-lease|diag|info|mac-vendor <WORD>|mem|noc diag|pm|process|
reboot-history|rf-domain-manager|snmp session|startup-log|sysinfo||top|
upgrade-history|watchdog|wireless|xpath-history]

service show advanced-wips stats [ap-table|client-table|connected-sensors-
status|termination-entries]

service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}
service show [command-history|crash-info|info|mem|startup-
log|process|sysinfo|top|upgrade-history|watchdog] {on <DEVICE-NAME>}

service show dhcp-lease {<WORD>|on|vlan>}
service show dhcp-lease <WORD> {on <DEVICE-NAME>}
service show dhcp-lease {on <DEVICE-NAME>}
service show dhcp-lease vlan <1-4094> {on <DEVICE-NAME>}

service show diag [led-status|stats] {on <DEVICE-NAME>}

service show pm {history|on <DEVICE-NAME>}
service show pm history  {on <DEVICE-NAME>}

service show rf-domain-manager diag {<DEVICE-NAME|on>}
service show rf-domain-manager diag <DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}
service show rf-domain-manager diag {on <DEVICE-OR-DOMAIN-NAME>}



service show wireless [client|config-internal|credential-cache|neighbors|stats-
client|vlan-usage]

service show wireless client proc [info|stats]
service show wireless client proc [info|stats] {<MAC>|on}
service show wireless client proc [info|stats] <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
service show wireless client [info|stats] {on <DEVICE-OR-DOMAIN-NAME>}

service show wireless config-internal {include-factory}]]
service show wireless stats-client diag {<DEVICE-NAME>|on}
service show wireless stats-client diag <DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>
service show wireless stats-client diag {on <DEVICE-OR-DOMAIN-NAME>}

service smart-rf [clear-config|clear-history|interactive-calibration|interactive-
calibration-result|run-calibration|stop-calibration]
```

```
service smart-rf [clear-config|clear-history|interactive-calibration|run-
calibration|stop-calibration]{on <DOMAIN-NAME>}
service smart-rf interactive-calibration-result [discard|replace-current-
config|write-to-configuration]{on <DOMAIN-NAME>}

service wireless [client|dump-core-snapshot|qos|wips]
service wireless client beacon-request <MAC> mode [active|passive|table]ssid
[<WORD>|any] channel-report [<WORD>|none]{on <DEVICE-NAME>}
service wireless qos  delete-tspec  <AA-BB-CC-DD-EE-FF> tid <0-7>
service wireless wips [clear-event-history|clear-client-blacklist]
service wireless wips clear-client-blacklist [all|mac <AA-BB-CC-DD-EE-FF>
service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME>}
]
```

Syntax Privilege Exec Mode

```
service [advanced-wips|clear|cli-tables-expand|cli-tables-
skin|cluster|copy|locator|mint|noc|pktcap|pm|radio|set|show|signal|smart-rf|start-
shell||wireless]
service copy tech-support [FILE|URL]
service clear [ap-upgrade|command-history|crash-info|noc|reboot-
history|unsanctioned|upgrade-history|wireless]
service mint [clear lsp-db|expire lsp|flood [csnp|lsp]|silence]
service signal [abort <WORD>|kill <WORD>]
service pm stop{on <DEVICE-NAME>}
service show [advanced-wips|captive-portal|cli|command-history|
crash-info|dhcp-lease|diag|info|last-passwd|mac-vendor|mem|noc|pm|process|reboot-
history|rf-domain-manager|snmp|startup-log|sysinfo||top|upgrade-
history|watchdog|wireless|
xpath-history]
```

Syntax Global Config Mode

```
service [set|show cli]
service set [command-history <10-300>|upgrade-history <10-100>|
reboot-history <10-100>] {on <DEVICE-NAME>}
```

NOTE: The parameters of the 'service' command of (User Exec, Privileged Exec, Global Config) are documented separately in 'Parameter Tables'.

Parameters

advanced-wips [clear-event-history {accidental-association|| crackable-wep-iv-used|dos-cts-flood| dos-deauthentication-detection|dos-disassociation-detection|dos-eap-failure-spoof| dos-eapol-logoff-storm|dos-rts-flood| essid-jack-attack-detected| fake-dhcp-server-detected|fata-jack-detected| id-theft-eapol-success-spoof-detected| id-theft-out-of-sequence| invalid-channel-advertized|invalid-management-frame| ipx-detection|monkey-jack-attack-detected| multicast-all-routers-on-subnet| multicast-all-systems-on-subnet| multicast-dhcp-server-relay-agent|multicast-hsrp-agent|multicast-igmp-detection| multicast-igrp-routers-detection| multicast-ospf-all-routers-detection| multicast-ospf-designated-routers-detection| multicast-rip2-routers-detection|	Advanced-WIPS Commands • clear-event-history – Clears the event history • accidental-association – Accidental client association • crackable-wep-iv-used – Crackable WEP IV Used • dos-cts-flood – DoS CTS flood • dos-deauthentication-detection – Detects DoS deauthentication • dos-disassociation-detection – Detects DoS disassociation • dos-eap-failure-spoof – Detects DoS EAP failure spoof • dos-eapol-logoff-storm – Detects DoS EAPoL logoff storm • dos-rts-flood – Detects DoS RTS flood • essid-jack-attack-detected – Detects ESSID jack attacks • fake-dhcp-server-detected – Detects fake DHCP server • fata-jack-detected – Detects fata-jack attacks • id-theft-eapol-success-spoof-detected – Detects IDs theft - EAPOL success spoof • id-theft-out-of-sequence – Detects IDs theft - out of sequence • invalid-channel-advertized – Detects invalid channel advertizement • invalid-management-frame – Detects invalid management frames • ipx-detection – Detects IPX • monkey-jack-attack-detected – Detects monkey-jack attacks • multicast-all-routers-on-subnet – Detects all multicast routers on the subnet • multicast-all-systems-on-subnet – Detects all multicast systems on the subnet • multicast-dhcp-server-relay-agent – Detects multicast DHCP server relay agents • multicast-hsrp-agent – Detects multicast HSRP agents • multicast-igmp-detection – Detects multicast IGMP • multicast-igrp-routers-detection – Detects multicast IGRP routers • multicast-ospf-all-routers-detection – Detects multicast OSPF all routers • multicast-ospf-designated-routers-detection – Detects multicast OSPF designated routers • multicast-rip2-routers-detection – Detects multicast RIP2 routers • multicast-vrrp-agent – Detects multicast VRRP agents • netbios-detection – Detects NetBIOS • null-probe-response-detected – Detects null probe response • probe-response-flood – Detects probe response flood • rogue-ap-detection – Detects rogue AP • stp-detection – Detects STP
multicast-vrrp-agent|netbios-detection|null-probe-response-detected|probe-response-flood|rogue-ap-detection|stp-detection	• unauthorized-bridge – Unauthorized bridge detection • windows-zero-config-memory-leak – Detects windows zero config memory leak • wlan-jack-attack-detected – Detects WLAN jack attacks

unauthorized-bridge|windows-zero-config-memory-leak|wlan-jack-attack-detected}|terminate-device <MAC>]	• terminate-device <MAC> – Terminates an AP or client • <MAC> – MAC address of AP or client
cli-tables-expand {left|right}	Expands CLI table in drop down format • left – Left justify output line • right – Right justify output line
cli-tables-skin [ansi|hashes|minimal|none|percent|stars|thick|thin|uf-8] {grid}	Chooses a formatting layout/skin for CLI tabular outputs • ansi – Uses ANSI characters for borders • hashes – Uses hashes (#) for borders • minimal – Minimal, (one horizontal line between title and data rows) • none – Space separated items, no decoration • percent – Uses the percent sign (%) for borders • stars – Use asterisks (*) for borders • thick – Uses thick lines for borders • thin – Uses thin lines for borders • utf-8 – Uses UTF-8 characters for borders • grid – Optional. Uses a complete grid instead of title lines
cluster manual-revert	Cluster Protocol • manual-revert – Triggers manual revert on a standby controller
locator {on <DEVICE-NAME>}	Enables LEDs flashing on the device • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – Displays AP/Controller information
noc parallel-updates <1-1024>	Configures NoC controller serviceability commands • parallel-updates <1-1024> – Sets the number of parallel threads limit from 1 to 1024

pktcap on [bridge|deny| drop|ext-vlan|interface| radio|rim|router|vpn| |wireless] {acl-name <WORD>| count <1-1000000> |direction|filter|hex| rate <1-100>| snap <1-2048>| tcpdump|verbose|write [file|url|tzsp]}	Starts the packet capture • on – Enter the capture location from the list • bridge – Captures packets transiting through the ethernet bridge • deny – Captures packets denied by an ACL • drop – Captures packets at drop locations • ext-vlan – Captures packets forwarded to/from an extended VLAN • interface {<WORD>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>} – Captures packets at a specified interface • <WORD> – Enter the interface name to capture packets • ge <1-4> – GigabitEthernet interface from 1-4 • me1 – FastEthernet interface • port-channel <1-2> – Select a port-channel interface index from 1-2 • vlan <1-4094> – Select a vlan id from 1-4094 • radio [<1-3>|all] – Captures on a radio (802.11) • <1-3> – Select a radio index from 1-3 • all – Selects all radios • rim – Captures packets at radio interface module • router – Captures packets transiting through IP router • vpn – Captures packets forwarded to/from a VPN link • wireless – Capture packets forwarded to/from wireless The following parameters are common for the above: • acl-name <WORD> – Specify the ACL that matches the acl-name for 'deny' location • count <1-1000000> – Captures packet count from 1-1000000 • direction [any|inbound|outbound] – Changes the packet direction with respect to a device • any – Any direction • inbound – Inbound direction • outbound – Outbound direction • filter <LINE> – Captures filter (must be last option) • <LINE> – Defines user defined packet capture filter • hex – Provides binary output • rate <1-100> – Specifies the rate at which the packets are captured per second • snap <1-2048> – Captures the data length • tcpdump – Decodes with TCP dump • verbose – Provides verbose output

	• write – Captures a file at a specified location • FILE Files: flash:/path/file cf:/path/file usb1:/path/file usb2:/path/file nvram:startup-config • URL – URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>@<hostname|IP>[:port]>/path/file • tzsp – Tazman Sniffer Protocol Host
radio <1-3> [data-rates rate-index <0-27> [basic|supp]| dfs simulate-radar [extension|primary]	Configures radio parameters • <1-3> – Index value between 1 and 3 • data-rates rate-index <0-27> – Configures radio data rates • rate-index <0-27> [basic|supp] – Specify a rate index between 0 and 27 • basic – Specifies basic rates • supp – Specifies supported rates • dfs simulate-radar – Configures DFS related serviceability commands • simulate-radar [extension|primary] – Simulates the presence of radar on a channel • extension – Simulates the presence of radar on the radios current extension channel • primary – Simulates the presence of radar on the radios current primary channel
set validation-mode [full|partial] {on <DEVICE-NAME>}	Sets validation mode • validation-mode [full|partial] – Displays the mode used to validate configuration settings • full {on <DEVICE-NAME>} – Uses full configuration validation • partial {on <DEVICE-NAME>} – Uses partial configuration validation bypass) • {on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – Specifies the AP/Controller name

show [advanced-wips|captive-portal|cli|command-history|crash-info|dhcp-lease|diag|info| mac-vendor <WORD>| mem|noc|pm|process| reboot-history| rf-domain-manager diag {on <DEVICE-NAME>}| snmp|startup-log| sysinfo||top| upgrade-history| watchdog|wireless| xpath-history]	Displays the statistics about the running system
	• advanced-wips stats [ap-table|client-table|connected-sensors-status|termination-entries] – Displays advanced-wips settings
	  • stats – Displays advanced-wips statistics
	  • ap-table – AP table
	  • client-table – Client table
	  • connected-sensors-status – Connected sensors
	  • termination-entries – Termination entries
	• captive-portal[servers|user-cache] – Displays captive portal commands
	  • servers {on <DEVICE-NAME>} – Displays server information for active captive portals
	  • user-cache {on <DEVICE-NAME>} – Displays cached user details for a captive portal
	• command-history {on <DEVICE-NAME>} – Displays command history
	• crash-info {on <DEVICE-NAME>} – Displays information about core, panic and AP dump files
	• dhcp-lease {<WORD>|on|vlan} – Displays DHCP lease information received from the server
	  • <WORD> on <DEVICE-NAME> – Specify the interface name
	  • on <DEVICE-NAME> – On AP/Controller
	  • vlan <1-4094> on <DEVICE-NAME> – Specify a VLAN index between 1 and 4094
	  • on <DEVICE-NAME> – On AP/Controller
	  • <DEVICE-NAME> – AP/Controller name
	• diag [led-status|stats] {on <DEVICE-NAME>} – Displays service show diag statistics commands
	  • led-status – Displays LED's system status
	  • stats – Displays system fan speed and sensor temperature
	• info {on <DEVICE-NAME>} – Displays snapshot of available support information
	• mem {on <DEVICE-NAME>} – Displays the system's current memory usage
	• noc diag – Displays information regarding noc diagnostics
	• pm {history|on <DEVICE-NAME>} – Displays information about process controlled by Process Monitor
	  • history {on <DEVICENAME>} – Displays state changes for a process
	• process {on <DEVICENAME>} – Displays active system process information
	• reboot-history {on <DEVICE-NAME>} – Displays the reboot history

	• rf-domain-manager diag {<DEVICE-NAME>|on} – Displays the RF Domain manager information • diag {<DEVICE-NAME|on>} – Displays diagnostic information about RF Domain manager • <DEVICE-NAME> on <DEVICE-OR-DOMAIN-NAME> – Specify the MAC address of the device or its hostname • on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/RF Domain • snmp session – Displays information regarding SNMP • session – Displays SNMP session information • startup-log {on <DEVICE-NAME>} – Displays the startup log • sysinfo {on <DEVICE-NAME>} – Displays the system's memory usage • upgrade-history {on <DEVICE-NAME>} – Displays the upgrade history of the specified device • xpath-history {on <DEVICE-NAME>} – Displays the xpath history of the specified device • top {on <DEVICE-OR-DOMAIN-NAME>} – Displays system resource information • watchdog {on <DEVICE-NAME>} – Displays watchdog status • wireless [client|config-internal|credential-cache|neighbors|stats-client|vlan-usage] – Displays wireless commands • client proc – Displays proc-entries for clients • proc [info|stats] – Dataplane proc entries • info {<MAC>| on} – Displays information about clients • stats {<MAC>|on} – Displays statistics about clients • <MAC> {on <DEVICE-OR-DOMAIN-NAME> – Specify the MAC address of the client device • on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller • config-internal include-factory – Displays selected internal configuration parameters • include-factory – Includes factory default values • credential-cache – Displays the cached credentials (keys, vlan etc) of wireless clients • neighbors – Displays devices considered for neighbors, roaming and flow migration • stats-client diag – Displays information regarding managed Access Points • diag {<DEVICE-NAME>|on} – Displays diagnostic information about wireless AP • vlan-usage – Displays usage of VLANs across currently in-use wireless LANs • cli – Displays the CLI tree of current mode • mac-vendor <WORD> – Displays the vendor name for a given MAC address or OUI portion of a MAC address

	• noc diag – Displays information regarding noc updates
	  • diag – Diagnostic information
	• pm [history|all] – Displays information about the processes controlled by process monitor
	  • history – Displays the state changes for a process
	  • on – On AP/Controller
	  • <WORD> {on <DEVICE-NAME>} – Enter the process name
	  • all {on <DEVICE-NAME>} – All processes

smart-rf [clear-config| clear-history |interactive-calibration |run-calibration| stop-calibration |interactive-calibration-result]	Smart-RF Management Commands
	• clear-config {on <DOMAIN-NAME>} – Clears the Smart RF configuration on all devices
	• clear-history {on <DOMAIN-NAME>} – Clears the Smart RF history on all devices
	• interactive-calibration {on <DEVICE-NAME>} – Interactive Smart RF calibration
	• run-calibration {on <DEVICE-NAME>} – Starts a new calibration process
	• stop-calibration {on <DEVICE-NAME>} – Stops the calibration currently in progress
	• interactive-calibration-result [discard|replace-current-config|write-to-configuration] – Specifies interactive smart-rf calibration result
	  • discard {on <DOMAIN-NAME>} – Discards interactive calibration results
	  • replace-current-config {on <DOMAIN-NAME>} – Replaces current radio configuration
	  • write-to-configuration {on <DOMAIN-NAME>} – Writes and saves radio settings to configuration
	The following are the same for the above parameters:
	• on <DOMAIN-NAME> – On RF Domain
	  • <DOMAIN-NAME> – RF Domain name

clear [ap-upgrade| command-history|noc| reboot-history| upgrade-history| unsanctioned|wireless]	Performs a variety of reset functions • command-history {on <DEVICE-NAME>} – Clears the command history • reboot-history {on <DEVICE-NAME>} – Clears the reboot history • upgrade-history {on <DEVICE-NAME>} – Clears the upgrade history The following is common for the above: • {on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – AP/Controller name • ap-upgrade history – Clears the AP upgrade history • noc statistics – Clears noc related serviceability commands • statistics – Clears applicable statistics counters • unsanctioned – Clears unsanctioned AP detection service commands • aps – Clears the list of all the unsanctioned APs detected • {on <DEVICE-OR-DOMAIN-NAME>} – On AP/Controller • <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF Domain name • wireless [ap|client|radio|wlan] – Clears the wireless commands • ap statistics – Clears wireless AP related serviceability commands • statistics {<MAC>|on} – Clears applicable AP statistics counters • client statistics – Clears wireless client related serviceability commands • statistics {<MAC>|on} – Clears applicable client statistics counters The following are common for wireless ap and wireless client: • {<MAC> on <DEVICE-OR-DOMAIN-NAME>} – Specify the MAC address of a particular wireless client • {on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/ RF Domain • <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF Domain name • radio statistics – Clears wireless radio related serviceability commands • statistics {<DEVICE-NAME>|on} – Clears applicable radio statistics counters • <DEVICE-NAME> {<1-3>|on} – Specify the hostname or MAC address • <1-3> {on <DEVICE-OR-DOMAIN-NAME>} – Specifies the radio interface index if not specified as part of radio ID • on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/ RF Domain name • wlan statistics – Clears wireless WLAN related serviceability commands • statistics {<WLAN>|on} – Clears applicable WLAN statistics counters

	• <WLAN> {on <DEVICE-OR-DOMAIN-NAME>} – Specify a WLAN name • {on <DEVICE-OR-DOMAIN-NAME>} – On AP/Controller or RF Domain • <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF Domain name
wireless [client|dump-core-snapshot|qos|wips]	Configures wireless service commands • client beacon-request <MAC> mode [active|passive|table] ssid [<WORD>|any] channel-report[<WORD>|none] {on <DEVICE-NAME>} – Configures wireless client service commands • beacon-request <MAC> – Sends an 802.11k Beacon Measurement Request to a specified client • <MAC> mode – Enter the MAC address of the client • mode [active|passive|table] – Specify the mode in which the client must make the measurement • active – Requests the client to make the measurement in active mode • passive – Requests the client to make the measurement in passive mode • table – Requests the client to make the measurement in table mode The following are common for the active, passive, and table sub-commands • ssid[<WORD>|any] – Specify an SSID for which the measurements must be made • [<WORD>|any] channel-report – Specify a particular SSID or any SSID • channel-report[<WORD>|none] – Configures channel report in the request • <WORD> {on <DEVICE-NAME>} – Specify a comma separated list of channels • none {on <DEVICE-NAME>} – Applies to all channels • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – Specifies the AP/Controller name • dump-core-snapshot – Triggers a debug core-dump of the wireless module • qos – Wireless QoS related serviceability commands • delete-tspec <AA-BB-CC-DD-EE-FF> – Sends a DELETE-TSPEC message to a specified client

]]	• <AA-BB-CC-DD-EE-FF> rid – Enter the client MAC address • tid <0-7> – Enter the traffic identifier from 0-7 • wips [clear-event-history | clear-client-blacklist [all|mac <AA-BB-CC-DD-EE-FF>] – Configures WIPS service commands • clear-event-history {on <DEVICE-OR-DOMAIN-NAME> – Clears the event history
	• on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller • <DEVICE-OR-DOMAIN-NAME> – Specifies AP/Controller/RF Domain name • clear-client-blacklist [all|mac <AA-BB-CC-DD-EE-FF>] – Clears the client information from blacklist • all – Clears all clients from blacklist • mac <AA-BB-CC-DD-EE-FF> – Clears a specific client from the blacklist • <AA-BB-CC-DD-EE-FF> – Enter a client MAC address

ParametersPrivilege Exec Mode

copy tech-support [FILE|URL]	Copies files for technical support
	• tech-support [<file>|<URL>] [tftp|ftp|sftp] – Copies extensive system information useful to technical support for troubleshooting
	  • FILE – File to which to copy
	  • cf:/path/file
	  • usb1:/path/file
	  • usb2:/path/file
	  • URL– Target URL from which to copy
	  • tftp://<hostname:port or IP>/path/file
	  • ftp://<user>:<passwd>@ <hostname:port or IP>/path/file
	  • sftp://<user>@<hostname:port or IP>/path/file

clear [ap-upgrade| command-history|crash-info|noc| reboot-history| unsanctioned| upgrade-history|wireless]	Same as 'User Exec' mode 'service clear' parameters except the crash-info parameter
	• crash-info {on <DEVICE-NAME>} – Clears all crash files
	  • {on <DEVICE-NAME>} – On AP/Controller
	  • <DEVICE-NAME> – AP/Controller name

mint [clear lsp-db|expire lsp|flood[csnp|lsp]|silence]	Configures MiNT protocol parameters
	• clear lsp-db – Resets functions
	  • lsp-db – Clears the MiNT LSB database
	• expire lsp – Forces expiration
	  • lsp – Forces expiration of the LSP
	• flood[csnp|lsp] – Flood control packet
	  • csnp – Floods our CSNP
	  • lsp – Flood our LSP
	• silence – Run silent

pm stop {on <DEVICE-NAME>}	Process Monitor
	• stop – Stops PM from monitoring all daemons
	  • {on <DEVICE-NAME>} – On AP/Controller
	  • <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF Domain name

start-shell	Provides shell access

signal [abort <WORD>|kill <WORD>]	Sends a signal to a process • abort <WORD> – Sends an abort signal (to force it to dump core) • kill <WORD> – Sends a kill signal (terminate without a core) • < WORD> – Enter the name of process to be signalled
show [advanced-wips|captive-portal|cli|command-history|crash-info|dhcp-lease|diag|info|last-passwd|mac-vendor <WORD>|mem|noc|pm|process|reboot-history|rf-domain-manager|snmp|startup-log|sysinfo||top|upgrade-history|watchdog|wireless|xpath-history]	Same as 'User Exec' Mode 'service show' parameters except 'last-passwd' parameter • last-passwd – Displays the last password used to enter the shell service

ParametersGlobal Config Mode

set [command history <10-300>|upgrade history <10-100>|reboot history <10-100>] {on <DEVICE-NAME>}	Defines validation mode settings
	• command history <10-300> – Sets the size of command history. The default size is 200)
	• reboot history <10-100> – Sets the size of the reboot history. The default size is 50.
	• upgrade history <10-100> – Sets the size of the upgrade history. The default size is 50.
	  • {on <DEVICE-NAME>} – On AP/Controller
	  • <DEVICE-NAME> – AP/Controller name

show cli	Displays running system configuration • cli – Displays the CLI tree of the current mode

Example

```
rfs7000-37FABE>service cli-tables-skin stars
rfs7000-37FABE>

rfs7000-37FABE>service pktcap on interface vlan 2
Capturing up to 50 packets. Use Ctrl-C to abort.

rfs7000-37FABE>service show cli
User Exec mode:  +-do
+-help [help]
  +-show
    +-configuration-tree [help show configuration-tree]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show)]
      +-detailed [help search WORD (|detailed|only-show|skip-show)]
      +-only-show [help search WORD (|detailed|only-show|skip-show)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show)]
+-show
```

```
  +-commands [show commands]
  +-running-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config) (|include-factory)]
    +-interface [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-
4094>') (|include-factory)]
      +-WORD [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-
4094>') (|include-factory)]
        +-include-factory [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-
4>|vlan <1-4094>') (|include-factory)]
      +-ge
        +-<1-4> [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-
4094>') (|include-factory)]
         +-include-factory [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-
4>|vlan <1-4094>') (|include-
factory)].....................................................................rfs7000-
37FABE>

rfs7000-37FABE>service show general stats on rfs7000-37FABE
Current Fan Speed: 6540 Minimum Fan Speed: TBD Hysteresis: TBD

Sensor 1 Temperature: 31C
Sensor 2 Temperature: 55C
Sensor 3 Temperature: 29C
Sensor 4 Temperature: 28C
Sensor 5 Temperature: 26C
Sensor 6 Temperature: 28C


rfs7000-37FABE>

rfs7000-37FABE>service wireless wips clear-mu-blacklist mac 11-22-33-44-55-66
rfs7000-37FABE>

rfs7000-37FABE#service signal kill testp
Sending a kill signal to testp
rfs7000-37FABE#
rfs7000-37FABE#service signal abort testprocess
Sending an abort signal to testprocess
rfs7000-37FABE#

rfs7000-37FABE#service mint clear lsp-db
rfs7000-37FABE#

rfs7000-37FABE#service mint silence
rfs7000-37FABE#

rfs7000-37FABE#service pm stop on rfs7000-37FABE
rfs7000-37FABE#

rfs7000-37FABE(config)#service show cli
Global Config mode:
+-help [help]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show)]
      +-detailed [help search WORD (|detailed|only-show|skip-show)]
      +-only-show [help search WORD (|detailed|only-show|skip-show)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show)]
+-show
  +-commands [show commands]
  +-eval
    +-LINE [show eval LINE]
  +-debugging [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]
    +-cfgd [show debugging cfgd]
    +-on
      +-DEVICE-OR-DOMAIN-NAME [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]
    +-wireless [show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))]
      +-on
       +-DEVICE-OR-DOMAIN-NAME [show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))]
    +-voice [show debugging voice (|(on DEVICE-OR-DOMAIN-NAME))]
      +-on
```

```
        +-DEVICE-OR-DOMAIN-NAME [show debugging voice (|(on DEVICE-OR-DOMAIN-NAME))]
    +-captive-portal [show debugging captive-portal (|(on DEVICE-OR-DOMAIN-NAME))]
      +-on
       +-DEVICE-OR-DOMAIN-NAME [show debugging captive-portal (|(on DEVICE-OR-DOMAIN-
NAME))]
    +-dhcpsvr [show debugging dhcpsvr (|(on DEVICE-NAME))]
      +-on.....................................................
rfs7000-37FABE(config)#

rfs7000-37FABE#service traceroute -h
traceroute: invalid option -- h
BusyBox v1.14.1 () multi-call binary

Usage: traceroute [-FIldnrv] [-f 1st_ttl] [-m max_ttl] [-p port#] [-q nqueries]
        [-s src_addr] [-t tos] [-w wait] [-g gateway] [-i iface]
        [-z pausemsecs] HOST [data size]

Trace the route to HOST

Options:
        -F      Set the don't fragment bit
        -I      Use ICMP ECHO instead of UDP datagrams
        -l      Display the ttl value of the returned packet
        -d      Set SO_DEBUG options to socket
        -n      Print hop addresses numerically rather than symbolically
        -r      Bypass the normal routing tables and send directly to a host
        -v      Verbose
        -m max_ttl      Max time-to-live (max number of hops)
        -p port#        Base UDP port number used in probes
                        (default is 33434)
        -q nqueries     Number of probes per 'ttl' (default 3)
        -s src_addr     IP address to use as the source address
        -t tos          Type-of-service in probe packets (default 0)
        -w wait         Time in seconds to wait for a response
                        (default 3 sec)
        -g              Loose source route gateway (8 max)

rfs7000-37FABE#

rfs7000-37FABE>ser show ap configured
------------------------------------------------------------------------------
 IDX       NAME              MAC             PROFILE       RF-DOMAIN       ADOPTED-BY
------------------------------------------------------------------------------  1
ap7131-889EC4   00-15-70-88-9E-C4   default-ap7131   default     un-adopted
2   ap650-445566    11-22-33-44-55-66   default-ap650    default     un-adopted
  3   ap650-000000    00-A0-F8-00-00-00   default-ap650    default    00-15-70-37-FA-BE
------------------------------------------------------------------------------rfs7000-
37FABE>

rfs7000-37FABE>service show command-history on rfs7000-37FABE
Configured size of command history is 200

Date & Time           User      Location           Command
==============================================================
Jul 28 16:39:34 2010   admin    172.16.10.10 17     service locator on rfs7000-37FABE
Jul 28 16:39:13 2010   admin     172.16.10.10 17      exit
Jul 28 16:17:51 2010   admin     172.16.10.10 17      exit
Jul 28 16:15:58 2010   admin     172.16.10.10 17      exit
Jul 28 16:15:53 2010   admin     172.16.10.10 17      advanced-wips-policy test
Jul 28 16:08:13 2010   admin     172.16.10.10 17      exit
Jul 28 15:24:25 2010   admin     172.16.10.10 16      firewall-policy test
Jul 28 13:51:59 2010   admin     172.16.10.10 15      exit
Jul 28 13:51:47 2010   admin     172.16.10.10 15      exit
Jul 28 13:51:44 2010   admin     172.16.10.10 15      exit
Jul 28 13:51:43 2010   admin     172.16.10.10 15      exit
Jul 28 13:21:17 2010   admin     172.16.10.10 15      aaa-policy test
Jul 28 13:20:35 2010   admin     172.16.10.10 15      exit
Jul 28 13:09:14 2010   admin     172.16.10.10 15      exit
Jul 28 13:08:44 2010   admin     172.16.10.10 15      aaa-policy test
Jul 27 13:46:46 2010   admin    172.16.10.10 6      ip nat pool pool1 prefix-length 1
```

```
Jul 27 13:44:46 2010   admin     172.16.10.10 6      profile rfs7000 default-rfs7000
Jul 27 12:39:29 2010   admin     172.16.10.12 5      reload force
Jul 27 12:28:41 2010   admin     172.16.10.12 20      reload force
Jul 27 12:28:39 2010   admin     172.16.10.12 20      write memory
.............................................................
rfs7000-37FABE>

rfs7000-37FABE>service show diag stats on rfs7000-37FABE

fan 1 current speed: 6660 min_speed: 2000 hysteresis: 250
fan 2 current speed: 6720 min_speed: 2000 hysteresis: 250
fan 3 current speed: 6540 min_speed: 2000 hysteresis: 250

Sensor 1 Temperature 32.0 C
Sensor 2 Temperature 58.0 C
Sensor 3 Temperature 29.0 C
Sensor 4 Temperature 28.0 C
Sensor 5 Temperature 26.0 C
Sensor 6 Temperature 28.0 C

rfs7000-37FABE>service show info on rfs7000-37FABE
7.7M out of 8.0M available for logs.
9.4M out of 10.0M available for history.
19.2M out of 20.0M available for crashinfo.

List of Files:

cfgd.log                                  5.7K    Jul 28 17:17
fmgr.log                                  221     Jul 27 12:40
messages.log                              1.0K    Jul 27 12:41
startup.log                               52.3K   Jul 27 12:40
command.history                           903     Jul 28 16:39
reboot.history                            1.6K    Jul 27 12:40
ugrade.history                            698     Jul 27 12:39

Please export these files or delete them for more space.

rfs7000-37FABE>
rfs7000-37FABE>service show upgrade-history on rfs7000-37FABE
Configured size of upgrade history is 50

  Date & Time             Old Version     New Version     Status
=====================================================================
Jul 27 12:37:30 2010 5.1.0.0-098D 5.1.0.0-097B Successful
Jul 27 12:26:34 2010 5.1.0.0-097B 5.1.0.0-098D Successful
Jul 22 16:33:04 2010 5.1.0.0-096B 5.1.0.0-097B Successful
Jul 22 16:32:15 2010 5.1.0.0-096B 5.1.0.0-096B Unable to get update file. ftpget:
cannot connect to remote host (172.16.10.1): Connection refused
Jul 19 17:51:29 2010 5.1.0.0-090D 5.1.0.0-096B Successful
Jul 12 12:41:12 2010 5.1.0.0-088D 5.1.0.0-090D Successful
Jul 06 12:38:49 2010 5.1.0.0-086D 5.1.0.0-088D Successful
Jun 29 13:06:50 2010 5.1.0.0-084D 5.1.0.0-086D Successful
.....................................................
rfs7000-37FABE
rfs7000-37FABE>service show watchdog
watchdog is enabled
countdown: 255 seconds of 260 remain until reset
rfs7000-37FABE>

rfs7000-37FABE>service show xpath-history
-------------------------------------------------------------------------------
-----------------------------------------
      DATE&TIME         USER                          XPATH
DURATION(MS)
-------------------------------------------------------------------------------
-----------------------------------------
 Wed Jul 28 17:29:49 2010  [system]  /wing-stats/device/00-A0-F8-00-00-00/_internal/
adjust_stats_interval   40
 Wed Jul 28 17:29:49 2010  [system]  /wing-stats/device/00-15-70-37-FA-BE/_internal/
adjust_stats_interval   16
```

```
  Wed Jul 28 17:29:43 2010   [system]   /wing-stats/device/00-A0-F8-00-00-00/_internal/
adjust_stats_interval   39
  Wed Jul 28 17:29:43 2010   [system]   /wing-stats/device/00-15-70-37-FA-BE/_internal/
adjust_stats_interval   16
  Wed Jul 28 17:29:37 2010   [system]   /wing-stats/device/00-A0-F8-00-00-00/_internal/
adjust_stats_interval   40
  Wed Jul 28 17:29:37 2010   [system]   /wing-stats/device/00-15-70-37-FA-BE/_internal/
adjust_stats_interval   17
  Wed Jul 28 17:29:31 2010   [system]   /wing-stats/device/00-A0-F8-00-00-00/_internal/
adjust_stats_interval   40
  Wed Jul 28 17:29:31 2010   [system]   /wing-stats/device/00-15-70-37-FA-BE/_internal/
adjust_stats_interval   16
  Wed Jul 28 17:29:30 2010   [system]   /wing-stats/device/00-15-70-37-FA-BE/watchdog-
status                   6

rfs7000-37FABE#service show last-passwd
Last password used: password with MAC 00:15:70:37:fa:be
rfs7000-37FABE#

rfs7000-37FABE>service show wireless ap diag on rfs7000-37FABE
--------------------------------------------------------------------------------
           AP-MAC                          FIELD                        VALUE
--------------------------------------------------------------------------------
  00-15-70-37-FA-BE          is_manager                    True
  00-15-70-37-FA-BE          last_stats_upload             107802.617188
  00-15-70-37-FA-BE          manager_mint_id               70.37.FA.BE
  00-15-70-37-FA-BE          max_pull_time                 2.80668640137
  00-15-70-37-FA-BE          num_adoptions                 0
  00-15-70-37-FA-BE          num_config_applied            0
  00-15-70-37-FA-BE          num_config_failed             0
  00-15-70-37-FA-BE          num_config_received           0
  00-15-70-37-FA-BE          num_stats_pulled              17951
  00-15-70-37-FA-BE          num_stats_pushed              0
  00-15-70-37-FA-BE          upload_state                  master
--------------------------------------------------------------------------------
--------------------------------------------------------------     AP-MAC
FIELD                      VALUE
--------------------------------------------------------------------------------
  00-A0-F8-00-00-00          is_manager                    False
  00-A0-F8-00-00-00          last_stats_upload             449767.65625
  00-A0-F8-00-00-00          manager_mint_id               70.37.FA.BE
  00-A0-F8-00-00-00          max_pull_time                 0
  00-A0-F8-00-00-00          num_adoptions                 2
  00-A0-F8-00-00-00          num_config_applied            2
  00-A0-F8-00-00-00          num_config_failed             0
  00-A0-F8-00-00-00          num_config_received           2
  00-A0-F8-00-00-00          num_stats_pulled              74796
  00-A0-F8-00-00-00          num_stats_pushed              3
  00-A0-F8-00-00-00          upload_state                  connected
--------------------------------------------------------------------------------
Total number of APs displayed: 2
rfs7000-37FABE>

rfs7000-37FABE>service show wireless config-internal
! Startup-Config-Playback Completed: Yes
no debug wireless
no country-code
!
wlan-qos-policy default
 no rate-limit wlan to-air
 no rate-limit wlan from-air
 no rate-limit client to-air
 no rate-limit client from-air
!
wlan wlan1
 ssid wlan1
 vlan 1
 qos-policy default
 encryption-type none
 authentication-type none
```

```
 no accounting radius
 no accounting syslog
rfs7000-37FABE>

System Information:

Free RAM:  68.0% (169 of 249)  Min: 10.0%
File Descriptors: free: 24198 used: 960 max: 25500
CPU load averages: 1 min: 0.0%  5 min: 0.0%  15 min: 0.0%

Kernel Buffers:
Size:      32    64   128   256   512    1k    2k    4k    8k   16k   32k   64k  128k
Usage:   2761  2965   927   201   549   107   141    25    68     0     1     2     0
Limit:  32768  8192  4096  4096  8192  8192 16384 16384  1024   512   256    64    64
rfs7000-37FABE#

rfs7000-37FABE>service clear wireless radio statistics on rfs7000-37FABE
clear radio stats on *: o.k.

rfs7000-37FABE#service show dhcp-lease vlan 1 on rfs7000-37FABE
No dhcp lease information available
rfs7000-37FABE#
```

5.1.9 write

Common Commands

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
write
```

Parameters

memory	Writes to NV memory
terminal	Writes to terminal

Example

```
rfs7000-37FABE>write memory
[OK]
rfs7000-37FABE>


rfs7000-37FABE>write terminal
!
! Configuration of RFS7000 version 5.1.0.0-061D
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 enable
 calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
 voice-prioritization
 svp-prioritization
 wmm background cw-max 8
 wmm video txop-limit 9
.....................................................................rfs7000-
37FABE>
```

CHAPTER 6 SHOW COMMANDS

This chapter provides an overview of all the show commands within the controller CLI structure.

This chapter describes the ' show ' CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

This chapter describes the 'show' commands in the 'GLOBAL CONFIG' mode. All the commands in this chapter can be entered in all the three modes except commands like file, ip-access-list-stats, mac-access-list-stats and upgrade stats commands, which cannot be entered in the User Executable Mode.

6.1 show commands

Table 6.1 Summarizes show commands

Table 6.1 *show commands*

Command	Description	Reference
show	Displays the settings for the specified system component	*page 6-5*
adoption	Displays information related to controller adoption	*page 6-8*
advanced-wips	Displays advanced-wips settings	*page 6-10*
ap-upgrade	Displays Access Point software image upgrade information	*page 6-13*
boot	Displays a device boot configuration	*page 6-14*
captive-portal	Displays WLAN hotspot functions	*page 6-15*
cdp	Displays a Cisco Discovery Protocol neighbor table	*page 6-17*
clock	Displays the software system clock	*page 6-18*
cluster	Displays cluster commands	*page 6-19*
commands	Displays command list	*page 6-20*
context	Displays information about the current context	*page 6-22*
critical-resources	Displays critical-resource information	*page 6-24*
crypto	Displays encryption mode information	*page 6-25*
debug	Displays debugging configuration information	*page 6-28*
debugging	Displays debugging configuration information	*page 6-30*
device-categorization	Displays device categorization details	*page 6-30*
event-history	Displays the event history	*page 6-33*
event-system-policy	Displays event system policy configuration information in detail	*page 6-34*

Table 6.1 *show commands*

Command	Description	Reference
file	Displays file system information	*page 6-35*
firewall	Displays wireless firewall information	*page 6-36*
interface	Displays the status of the different controller interfaces	*page 6-40*
ip	Displays Internet Protocol (IP) related information	*page 6-42*
ip-access-list-stats	Displays IP access list stats	*page 6-47*
licenses	Displays installed licenses and usage information	*page 6-48*
lldp	Displays Link Layer Discovery Protocol information on AP/ Controller	*page 6-49*
logging	Displays logging information	*page 6-50*
mac-access-list-stats	Displays MAC access list statistics	*page 6-51*
mac-address-table	Displays MAC address table entries	*page 6-52*
mint	Displays MINT protocol configuration commands	*page 6-53*
noc	Displays Noc-level information	*page 6-55*
ntp	Displays *Network Time Protocol* (NTP) information	*page 6-57*
password-encryption	Displays password encryption status information	*page 6-58*
power	Displays power over ethernet (PoE) information	*page 6-59*
remote-debug	Displays remote debug session data	*page 6-60*
rf-domain-manager	Displays RF Domain manager selection details	*page 6-61*
role	Displays role based firewall information	*page 6-62*
running-config	Displays the contents of configuration files	*page 6-63*

Table 6.1 *show commands*

Command	Description	Reference
session-changes	Displays the configuration changes made in this session	*page 6-65*
session-config	Displays the list of currently active open sessions on the device	*page 6-66*
sessions	Displays CLI sessions	*page 6-67*
smart-rf	Displays Smart RF Management commands	*page 6-68*
spanning-tree	Displays spanning-tree information	*page 6-70*
startup-config	Displays the complete startup configuration script on the console	*page 6-73*
terminal	Displays terminal configuration parameters	*page 6-74*
timezone	Displays the time zone	*page 6-75*
upgrade-status	Displays the status of the image upgrade	*page 6-76*
version	Displays the software and hardware version on the device	*page 6-77*
wireless	Displays wireless configuration parameters	*page 6-78*
wwan	Displays wireless WAN status	*page 6-85*

6.1.1 show

show commands

Displays settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances.
- When invoked with the display parameter, it displays information about that component.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show <parameter>
```

Parameters

None

Example

GLOBAL CONFIG Mode

```
rfs7000-37FABE(config)#show ?
  adoption                Display information related to adoption to wireless
                          controller
  advanced-wips           Advanced WIPS
  ap-upgrade              AP Upgrade
  boot                    Display boot configuration.
  captive-portal          Captive portal commands
  cdp                     Cisco Discovery Protocol
  clock                   Display system clock
  cluster                 Cluster Protocol
  commands                Show command lists
  context                 Information about current context
  critical-resources      Critical Resources
  crypto                  Encryption related commands
  debug                   Debugging functions
  debugging               Debugging functions
  device-categorization   Device Categorization
  event-history           Display event history
  event-system-policy     Display event system policy
  file                    Display filesystem information
  firewall                Wireless Firewall
  interface               Interface Configuration/Statistics commands
  ip                      Internet Protocol (IP)
  ip-access-list-stats    IP Access list stats
  licenses                Show installed licenses and usage
  lldp                    Link Layer Discovery Protocol
  logging                 Show logging information
  mac-access-list-stats   MAC Access list stats
  mac-address-table       Display MAC address table
  mint                    MiNT protocol
  noc                     Noc-level information
  ntp                     Network time protocol
  password-encryption     Pasword encryption
  power                   Show power over ethernet command
```

```
  remote-debug            Show details of remote debug sessions
  rf-domain-manager       Show RF Domain Manager selection details
  role                    Role based firewall
  running-config          Current operating configuration
  session-changes         Configuration changes made in this session
  session-config          This session configuration
  sessions                Display CLI sessions
  smart-rf                Smart-RF Management Commands
  spanning-tree           Display spanning tree information
  startup-config          Startup configuration
  terminal                Display terminal configuration parameters
  timezone                The timezone
  upgrade-status          Display last image upgrade status
  version                 Display software & hardware version
  wireless                Wireless commands
  wwan                    Display wireless WAN Status

rfs7000-37FABE(config)#
rfs7000-37FABE(config)#show clock
2011-04-30 09:28:29 GMT
```

PRIVILEGE EXEC Mode

```
rfs7000-37FABE#show ?
  adoption                Display information related to adoption to wireless
                          controller
  advanced-wips           Advanced WIPS
  ap-upgrade              AP Upgrade
  boot                    Display boot configuration.
  captive-portal          Captive portal commands
  cdp                     Cisco Discovery Protocol
  clock                   Display system clock
  cluster                 Cluster Protocol
  commands                Show command lists
  context                 Information about current context
  critical-resources      Critical Resources
  crypto                  Encryption related commands
  debug                   Debugging functions
  debugging               Debugging functions
  device-categorization   Device Categorization
  event-history           Display event history
  event-system-policy     Display event system policy
  file                    Display filesystem information
  firewall                Wireless Firewall
  interface               Interface Configuration/Statistics commands
  ip                      Internet Protocol (IP)
  ip-access-list-stats    IP Access list stats
  licenses                Show installed licenses and usage
  lldp                    Link Layer Discovery Protocol
  logging                 Show logging information
  mac-access-list-stats   MAC Access list stats
  mac-address-table       Display MAC address table
  mint                    MiNT protocol
  noc                     Noc-level information
  ntp                     Network time protocol
  password-encryption     Pasword encryption
  power                   Show power over ethernet command
  remote-debug            Show details of remote debug sessio
  rf-domain-manager       Show RF Domain Manager selection de
  role                    Role based firewall
  running-config          Current operating configuration
  session-changes         Configuration changes made in this
  session-config          This session configuration
  sessions                Display CLI sessions
  smart-rf                Smart-RF Management Commands
  spanning-tree           Display spanning tree information
  startup-config          Startup configuration
  terminal                Display terminal configuration para
  timezone                The timezone
  upgrade-status          Display last image upgrade status
```

```
  version                 Display software & hardware version
  wireless                Wireless commands
  wwan                    Display wireless WAN Status

rfs7000-37FABE#show terminal
rfs7000-37FABE#show terminal
Terminal Type: xterm
Length: 24     Width: 80
```

USER EXEC Mode

```
rfs7000-37FABE>show ?
  adoption                Display information related to adoption to wireless
                          controller
  advanced-wips           Advanced WIPS
  ap-upgrade              AP Upgrade
  captive-portal          Captive portal commands
  cdp                     Cisco Discovery Protocol
  clock                   Display system clock
  cluster                 Cluster Protocol
  commands                Show command lists
  context                 Information about current context
  critical-resources      Critical Resources
  crypto                  Encryption related commands
  debug                   Debugging functions
  debugging               Debugging functions
  device-categorization   Device Categorization
  event-history           Display event history
  event-system-policy     Display event system policy
  firewall                Wireless Firewall
  interface               Interface Configuration/Statistics commands
  ip                      Internet Protocol (IP)
  licenses                Show installed licenses and usage
  lldp                    Link Layer Discovery Protocol
  logging                 Show logging information
  mac-address-table       Display MAC address table
  mint                    MiNT protocol
  noc                     Noc-level information
  ntp                     Network time protocol
  password-encryption     Pasword encryption
  power                   Show power over ethernet command
  remote-debug            Show details of remote debug sessions
  rf-domain-manager       Show RF Domain Manager selection details
  role                    Role based firewall
  running-config          Current operating configuration
  session-changes         Configuration changes made in this session
  session-config          This session configuration
  sessions                Display CLI sessions
  smart-rf                Smart-RF Management Commands
  spanning-tree           Display spanning tree information
  startup-config          Startup configuration
  terminal                Display terminal configuration parameters
  timezone                The timezone
  version                 Display software & hardware version
  wireless                Wireless commands
  wwan                    Display wireless WAN Status
rfs7000-37FABE>show wireless ap configured
-------------------------------------------------------------------------
 IDX       NAME              MAC             PROFILE       RF-DOMAIN    ADOPTED-BY
-------------------------------------------------------------------------
1   ap7131-889EC4   00-15-70-88-9E-C4   default-ap7131   default    un-adopted
2   ap650-445566    11-22-33-44-55-66   default-ap650    default     un-adopted
-------------------------------------------------------------------------
rfs7000-37FABE>
```

6.1.2 adoption

show commands

Displays information related to controller adoption.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show adoption [config-errors <DEVICE-NAME>|history {on <DEVICE-NAME>}
|info|offline|pending]
```

Parameters

adoption [info|offline]	Displays the current adoption status of an access point
	• config-errors <DEVICE-NAME> – Displays the configuration errors of adopted access points
	  • <DEVICE-NAME> – On AP/Controller
	• info – Displays the adoption status of the device and its adopted access points
	• offline – Displays the unadopted status of the device and its adopted access points
	• history {on <DEVICE-NAME>} – Displays the adoption history status of the device and its adopted access points
	• pending {on <DEVICE-NAME>} – Displays the information related to non adopted access points
	  • on – On AP/Controller
	  • <DEVICE-NAME> – On AP/Controller

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#show adoption offline
------------------------------------------------------------------------
MAC               HOST-NAME           TYPE           RF-DOMAIN
------------------------------------------------------------------------
 00-15-70-88-9E-C4   ap7131-889EC4     ap7131           default
 11-22-33-44-55-66   ap650-445566      ap650          default
------------------------------------------------------------------------
Total number of APs displayed: 2
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#

rfs7000-37FABE(config-adoption-policy-test)#show adoption info
Number of APs adopted  : 1
Number of AAPs adopted : 0
Available AP licenses  : 49
Available AAP licenses : 50
Device in cluster      : No
Cluster state          : active
```

```
-------------------------------------------------------------------------------
MAC       HOST-NAME       TYPE    VERSION   ADOPTED-BY           LAST-ADOPTION
-------------------------------------------------------------------------------
00-A0-F8-00-00-00 ap650-000000 ap650  5.1.0.0-072RR   00-15-70-37-FA-BE   2010-08-17
23:48:48
-------------------------------------------------------------------------------
Total number of APs displayed: 1
rfs7000-37FABE(config-adoption-policy-test)#

rfs7000-37FABE(config)#show adoption history
-------------------------------------------------------------------------------
MAC          TYPE               EVENT             REASON            TIME-STAMP
-------------------------------------------------------------------------------  00-23-
68-13-9B-34  AP7131   adopted           N.A.   2011-01-01 05:28:14
-------------------------------------------------------------------------------
rfs7000-37FABE(config)#
```

6.1.3 advanced-wips

show commands

Displays advanced-wips settings.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show advanced-wips [configuration|stats]
show advanced-wips configuration [events {thresholds}|terminate-list]
show advanced-wips stats [ap-table|connected-sensors|detected-
aps{authorized|neighboring| unauthorized}|detected-stations-for-ap
<AA-BB-CC-DD-EE-FF>{authorized|neighboring|unauthorized}|
event-history|server-listening-port|client-table]
```

Parameters

configuration [events thresholds|terminate-list]	Displays advanced WIPS configuration details • events {thresholds} – Displays events summary • thresholds – Displays thresholds details • terminate-list – Displays the terminate list

stats [ap-table|connected-sensors|detected-aps{authorized|neighboring|unauthorized}|detected-stations-for-ap <AA-BB-CC-DD-EE-FF>{authorized|neighboring|unauthorized}|event-history|server-listening-port|client-table]	Displays advanced WIPS statistics details
	• ap-table – Displays the AP table
	• connected-sensors – Displays connected sensors information
	• detected-aps – Displays detected AP details
	  • authorized – Displays detected authorized AP information
	  • neighboring – Displays detected neighboring AP information
	  • unauthorized – Displays detected unauthorized AP information
	• detected-stations-for-ap – Displays detected clients for APs
	  • <AA-BB-CC-DD-EE-FF> – Enter the AP BSSID
	  • authorized – Displays detected authorized AP information
	  • neighboring – Displays detected neighboring AP information
	  • unauthorized – Displays detected unauthorized AP information
	• event-history – Displays the event history
	• server-listening-port – Displays server listening port information
	• client-table – Displays the station table

Example

```
rfs7000-37FABE(config)#show advanced-wips configuration events
+------+----+-------------------------------------------+----------+----
|POLICY|SLNO|                      NAME
|AUTHORIZED|UNAUTHORIZED|NEIGHBORING|
+------+----+-------------------------------------------+----------+----
| test | 1  | unauthorized-bridge                       | N        | N          | N        |
| test | 2  | dos-eapol-logoff-storm                    | N        | N          | N        |
| test | 3  | monkey-jack-attack-detected               | N        | N          | N        |
| test | 4  | dos-cts-flood                             | N        | N          | N        |
| test | 5  | crackable-wep-iv-used                     | N        | N          | N        |
| test | 6  | multicast-ospf-all-routers-detection      | N        | N          | N        |
| test | 7  | rogue-ap-detection                        | N        | N          | N        |
| test | 8  | fake-dhcp-server-detected                 | N        | N          | N        |
| test | 9  | multicast-vrrp-agent                      | N        | N          | N        |
| test | 10 | multicast-ospf-designated-routers-detection | N      | N          | N
|
| test | 11 | multicast-rip2-routers-detection          | N        | N          | N        |
| test | 12 | multicast-dhcp-server-relay-agent         | N        | N          | N        |
| test | 13 | id-theft-out-of-sequence                  | N        | N          | N        |
| test | 14 | stp-detection                             | N        | N          | N        |
| test | 15 | invalid-management-frame                  | N        | N          | N        |
| test | 16 | fata-jack-detected                        | N        | N          | N        |
| test | 17 | dos-deauthentication-detection            | N        | N          | N        |
```

```
| test | 18 | windows-zero-config-memory-leak          | N       | N        | N        |
| test | 19 | dos-eap-failure-spoof                    | N       | N        | N        |
| test | 20 | multicast-all-routers-on-subnet          | N       | N        | N        |
| test | 21 | essid-jack-attack-detected               | N       | N        | N        |
| test | 22 | dos-rts-flood                            | N       | N        | N        |
| test | 23 | accidental-association                   | N       | N        | N        |
| test | 24 | probe-response-flood                     | N       | N        | N        |
| test | 25 | invalid-channel-advertized               | N       | N        | N        |
| test | 26 | id-theft-eapol-success-spoof-detected    | N       | N        | N
|
| test | 27 | multicast-igmp-detection                 | N       | N        | N        |
| test | 28 | netbios-detection                        | N       | N        | N        |
| test | 29 | ipx-detection                            | N       | N        | N        |
| test | 30 | null-probe-response-detected             | N       | N        | N        |
| test | 31 | multicast-igmp-routers-detection         | N       | N        | N        |
| test | 32 | wlan-jack-attack-detected                | N       | N        | N        |
| test | 33 | multicast-hsrp-agent                     | N       | N        | N        |
| test | 34 | dos-disassociation-detection             | N       | N        | N        |
| test | 35 | multicast-all-systems-on-subnet          | N       | N        | N        |
| -    | -  | -                                        | -       | -        | -        |
+------+----+------------------------------------------+---------+----
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show advanced-wips configuration events thresholds
+--------+-----+--------------------------+--------------------------+----
| POLICY |  #  |          EVENT           |        THRESHOLD         |  VALUE  |
+--------+-----+--------------------------+--------------------------+----
| test   | 1   | dos-eapol-logoff-storm   | eapol-start-frames-ap    | 9       |
| test   | 2   | dos-eapol-logoff-storm   | eapol-start-frames-mu    | 99      |
| test   |3    | dos-cts-flood            | cts-frames-ratio         | 8       |
| test   |4    | dos-cts-flood            | mu-rx-cts-frames         | 20      |
| test   |5    | probe-response-flood     | probe-rsp-frames-count   | 50      |
| -      | -   | -                        | -                        | -       |
+--------+-----+--------------------------+--------------------------+----
rfs7000-37FABE(config)#


rfs7000-37FABE(config)#show advanced-wips stats detected-stations-for-ap 11-22-33-44-
55-66 authorized
Number of stations associated to the AP 11-22-33-44-55-66: 0
rfs7000-37FABE(config)#


rfs7000-37FABE(config)#show advanced-wips stats client-table
Number of clients: 2
rfs7000-37FABE(config)#
```

6.1.4 ap-upgrade

show commands

Displays Access Point software image upgrade information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show ap-upgrade [history|status {on rf-domain-manager}|versions {on rf-domain-manager}]
```

Parameters

history|status {on rf-domain-manager}|versions {on rf-domain-manager}	• history – Displays the history of an AP • status – Displays the status of an AP • versions – Displays the list of available upgrade images on all the Controllers

Example

```
rfs7000-37FABE(config)#show ap-upgrade history
------------------------------------------------------------------------------ AP
RESULT          TIME          RETRIES LAST UPDATE ERROR      UPGRADED BY
------------------------------------------------------------------------------
00-A0-F8-00-00-01   done   Nov 22 08:44:09 2010  0       -     00-15-70-37-FA-BE
00-A0-F8-00-00-10   done   Dec 05 05:20:14 2010   0  -        00-15-70-37-FA-BE
------------------------------------------------------------------------------
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ap-upgrade versions
------------------------------------------------------------------------------
 CONTROLLER                    AP-TYPE                  VERSION
------------------------------------------------------------------------------
 00-15-70-37-FA-BE             ap650               5.1.0.0-072R
 00-15-70-37-FA-BE             ap7131              none
 00-15-70-37-FA-BE             ap6511              none
------------------------------------------------------------------------------
rfs7000-37FABE(config)#
```

6.1.5 boot

show commands

Displays the boot configuration of a device. Use the 'on' command to view the boot configuration on a remote device.

NOTE: This command is not present in the USER EXEC Mode.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show boot {on <DEVICE-NAME>}
```

Parameters

boot {on <DEVICE-NAME>}	Displays boot information of a selected device

Example

```
rfs7000-37FABE(config)#show boot on rfs7000-37FABE
+-----------+-------------------------+-------------------------+--------------+
|   IMAGE   |        BUILD DATE       |       INSTALL DATE      |   VERSION    |
+-----------+-------------------------+-------------------------+--------------+
| Primary   | 03:26:2010 09:57:35 UTC | 04:01:2010 11:01:13 UTC | 5.1.0.0-072R |
| Secondary | 03:17:2010 04:19:10 UTC | 03:18:2010 16:41:44 UTC | 5.1.0.0- |072R
+-----------+-------------------------+-------------------------+--------------+
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
rfs7000-37FABE(config)#
```

6.1.6 captive-portal

show commands

Displays WLAN hotspot information.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show captive-portal client {filter|on}
show captive-portal client filter {captive-portal|ip|state|vlan|wlan}
show captive-portal client filter captive-portal {CAPTIVE-PORTAL|not CAPTIVE-PORTAL}
show captive-portal client filter ip {<A.B.C.D>|not <A.B.C.D>}
show captive-portal client filter state [not[pending|success]
|pending|success]
show captive-portal client filter vlan [VLAN-ID|not VLAN-ID]
show captive-portal client filter wlan [WLAN|not WLAN]
show captive-portal client {on <DEVICE-OR-DOMAIN-NAME>} filter {captive-
portal|ip|state|vlan|wlan}
```

Parameters

client {filter|on}	Displays connected captive portal client information • filter {captive-portal|ip|state|vlan|wlan} – Specifies an additional selection filter for getting table values • {on <DEVICE-OR-DOMAIN-NAME>} {filter {captive-portal|ip|state|vlan|wlan} – On AP/Controller or RF Domain name The following are common for the above: • captive-portal {CAPTIVE-PORTAL|not CAPTIVE-PORTAL} – Displays clients on the selected captive portal • CAPTIVE-PORTAL – Specify captive-portal name • not CAPTIVE-PORTAL – Invert match selection • ip {<A.B.C.D>|not <A.B.C.D>} – Selection by IP address • <A.B.C.D> – Specify IP address • not <A.B.C.D> – Invert match selection • state [not[pending|success] |pending|success] – Selection based on state • pending – Clients redirected for authentication • success – Clients successfully authenticated • not [pending|suucess] – Invert match selection • vlan [VLAN-ID|not VLAN-ID]– Displays clients on given VLAN • VLAN-ID – Specify the VLAN number • not VLAN-ID – Invert match selection • wlan [WLAN|not WLAN] – Displays clients on given WLAN • WLAN – Specify the WLAN name • not WLAN – Invert match selection

Example

```
rfs7000-37FABE(config)#show captive-portal client on rfs7000-37FABE
Number of Hotspot Mobile-Units: 1
```

6.1.7 cdp

show commands

Displays Cisco Discovery Protocol (CDP) neighbor table

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show cdp neighbors {on <DEVICE-NAME>}
```

Parameters

neighbors {on <DEVICE-NAME>}	Displays the CDP neighbor table • {on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
 rfs4000-22CDAA(config)#sh cdp neighbors on rfs4000-22CDAA
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
------------------------------------------------------------------------ DEVICE ID
LPORT    TTL     CAPABILITY        PLATFORM             PORT ID
------------------------------------------------------------------------ Switch
ge1     170     R S I       cisco WS-C3560-24PS    FastEthernet0/2
------------------------------------------------------------------------
```

6.1.8 clock

show commands

Displays the software system clock

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show clock {on <DEVICE-NAME>}
```

Parameters

clock {on <DEVICE-NAME>}	• on – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE(config)#show clock on rfs7000-37FABE
Apr 09 13:49:48 UTC 2010
rfs7000-37FABE(config)#
```

6.1.9 cluster

show commands

Displays cluster related information.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show cluster [configuration|members|status]
```

Parameters

cluster [configuration|members detail|status]	• configuration – Displays cluster configuration parameters • members detail – Displays known cluster members information in detail • status – Displays cluster status information

Example

```
rfs7000-37FABE(config)#show cluster configuration
Cluster Configuration Information
 Mode                            : Active
 Number of peer(s)               : 0
 Auto revert                     : Disabled
 Auto revert interval (Mins)     : 5
 Controller AP license               : 0
 Controller AAP license              : 0
 Controller max AP adoption capacity : 1024

Cluster Runtime Information
 Cluster protocol version         : 1
 Cluster run state                : active
 Cluster AP license               : 0
 Cluster AAP license              : 0
 Controller AP count                  : 0
 Controller AAP count                 : 0
 Cluster AP count                 : 0
 Cluster AAP count                : 0
 Cluster max AP adoption capacity : 1024
 Number of connected peer(s)      : 0

rfs7000-37FABE(config)#show cluster members detail
+-------------+------------------+--------+--------+---------+----------|      ID |
MAC   |  MODE   |AP COUNT|AAP COUNT|AP LICENSE|AAP LICENSE|   VERSION    |
+-------------+------------------+--------+--------+---------+----------|
70.37.fa.be | 00-15-70-37-FA-BE | Active | 0      | 0       | 0        | 0         |
Unknown     |
+-------------+------------------+--------+--------+---------+----------+
```

6.1.10 commands

show commands

Displays available commands for the current mode.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show commands
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show commands
    help
  help search WORD (|detailed|only-show|skip-show)
  show commands
  show debugging (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging cfgd
  show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging voice (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging captive-portal (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging dhcpsvr (|(on DEVICE-NAME))
  show debugging mstp (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging advanced-wips
  show debugging vpn (|(on DEVICE-NAME))
  show debugging radius (|(on DEVICE-NAME))
  show (running-config|session-config) (|include-factory)
  show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>')
(|include-factory)
  show running-config wlan WLAN (|include-factory)
  show (running-config) device (self|DEVICE-NAME) (|include-factory)
  show session-changes
  show startup-config (|include-factory)
  show adoption info (|(on DEVICE-NAME))
  show adoption offline
  show licenses
  show password-encryption status
  show debug xpath get WORD (|WORD)
  show debug xpath count WORD
  show debug xpath list WORD
  show rf-domain-manager
  show timezone
  show event-history
  show ntp status
  show ntp associations (|detail)
  show device-categorization summary
  show wireless ap (|(on DEVICE-OR-DOMAIN-NAME))
  show wireless ap configured
  show wireless ap detail (|WORD)
  show wireless unsanctioned aps (|(on DEVICE-OR-DOMAIN-NAME))
  show wireless unsanctioned aps detailed (|(on DEVICE-OR-DOMAIN-NAME))
  show wireless unsanctioned aps statistics (|(on DEVICE-OR-DOMAIN-NAME))
```

```
  show wireless client (|(on DEVICE-OR-DOMAIN-NAME)) (|(filter {|(state (|not) (data-
ready|roaming))|(wlan (|not) WLAN)|(ip (|not) A.B.C.D)}))
  show wireless client detail AA-BB-CC-DD-EE-FF (|(on DEVICE-OR-DOMAIN-NAME))
  show wireless client statistics (|traffic) (|(on DEVICE-OR-DOMAIN-NAME))
  show wireless client statistics rf (|(on DEVICE-OR-DOMAIN-NAME))
.............................................
rfs7000-37FABE(config)#
```

6.1.11 context

show commands

Displays information about the current context

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`show context {include-factory|session-config {include-factory}}`

Parameters

context {include-factory|session-config include-factory}	• include-factory – Displays information (including factory default values) • session-config – Displays running system information

Example

```
rfs7000-37FABE(config)#show context include-factory
!
! Configuration of RFS7000 version 5.1.0.0-072R
!
! version 2.0
!
!
smart-rf-policy default
 no enable
 auto-assign detector
 auto-assign channel
 auto-assign power
 assignable-power 5Ghz min 1
 assignable-power 5Ghz max 20
 assignable-power 2.4Ghz min 1
 assignable-power 2.4Ghz max 20
 channel-list 5Ghz
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,157,161,
165
 channel-list 2.4Ghz 1,6,11
 channel-width 5Ghz 40Mhz
 channel-width 2.4Ghz 20Mhz
 smart-ocs-monitoring
 smart-ocs-monitoring off-channel-duration 5Ghz 50
 smart-ocs-monitoring off-channel-duration 2.4Ghz 50
 smart-ocs-monitoring frequency 5Ghz 6
 smart-ocs-monitoring frequency 2.4Ghz 6
 smart-ocs-monitoring sample-count 5Ghz 5
 smart-ocs-monitoring sample-count 2.4Ghz 5
 smart-ocs-monitoring extended-scan-frequency 5Ghz 5
 smart-ocs-monitoring extended-scan-frequency 2.4Ghz 5
 interference-recovery
 interference-recovery noise
 interference-recovery interference
 no interference-recovery retry-threshold
```

```
 interference-recovery channel-Controller-delta 5Ghz 20
 interference-recovery .....................
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show context session-config
!
! Configuration of RFS7000 version 5.1.0.0-072R
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 enable
 calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
 voice-prioritization
 svp-prioritization
 wmm background cw-max 8
 wmm video txop-limit 9
 wmm voice cw-min 6
 wmm voice cw-max 6
 rate-limit client to-air max-burst-size 3
 rate-limit client to-air red-threshold video 101
 rate-limit client from-air rate 55
 rate-limit client from-air max-burst-size 6
 rate-limit client from-air red-threshold background 100
 rate-limit client from-air red-threshold voice 1010
!.................................................
rfs7000-37FABE(config)#
```

6.1.12 critical-resources

show commands

Displays critical resource information. Critical resources are resources that are vital to the wellbeing of the controller managed network.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show critical-resources {on <DEVICE-NAME>}
```

Parameters

critical-resources {on <DEVICE-NAME>}	Displays critical resource information • on – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs4000-22CDAA(config)#sh critical-resources on rfs4000-22CDAA
-------------------------------------------------------------------------------CRITICAL
RESOURCE IP        VLAN          PING-MODE            STATE
-------------------------------------------------------------------------
172.168.1.103               1             arp-icmp             up
```

6.1.13 crypto

show commands

Displays encryption mode information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show crypto [ipsec|isakmp|key|pki]
show crypto [ipsec|isakmp] sa {on <DEVICE-NAME>}
show  crypto  key rsa {on <DEVICE-NAME>|public-key-detail {on <DEVICE-NAME>}
show crypto pki trustpoints {<WORD>  {on <DEVICE-NAME>}|all {on <DEVICE-NAME>}|on
<DEVICE-NAME>}
```

Parameters

[ipsec|isakmp] sa {on <DEVICE-NAME>}	• ipsec – Displays the IPSEC policy • isakmp – Displays the ISAKMP policy The following parameters are common for the above: • sa – All crypto ISAKMP security associations • on – Displays ISAKMP security associations on AP/Controller • <DEVICE-NAME> – Displays AP/Controller name
key rsa {on <DEVICE-NAME>|public-key-detail {on <DEVICE-NAME>}	Displays key management operations • rsa – Displays RSA public keys • on <DEVICE-NAME> – On AP/Controller • public-key-detail {on} <DEVICE-NAME> – Displays the public key in PEM format • <DEVICE-NAME> – Displays the AP/ Controller name
pki trustpoints {<WORD> {on <DEVICE-NAME>}|all {on <DEVICE-NAME>}|on <DEVICE-NAME>}	Displays Public Key Infrastructure related commands • trustpoints – Displays configured trustpoints • <WORD> – Displays a particular trustpoint's information in detail • all – Displays details for all trustpoints • {on} <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – Displays AP/ Controller name

Example

```
rfs7000-37FABE(config)#show crypto key rsa public-key-detail on rfs7000-37FABE

RSA key name: default-trustpoint-srvr-priv-key   Key-length: 1024
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGHBR2bxLeRZ4G6hm7jHJRSaeE
A216r4s4qptiSld+rKeMihPTFbYELedk3dITkzF1EU7Ov0vKzant0pyAmdJ8ci//
wSQMmZjX3RwF9OFBRp2C09LFj/1VX2fsoD6xXhJHBLieJ9qzF+ZQ2CYG7+r29P/o
3rfr/GLaTN3C6RIWvQIDAQAB
-----END PUBLIC KEY-----


RSA key name: default_rsa_key        Key-length: 1024
-----BEGIN PUBLIC KEY-----
MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQCwXXWGE9j/i3EiSjnY9x1Ktsbt
rzgqB1KhlShWIgnWqlxjzvO6SvGmBPG5XqBS3rKqIzrgh6fXF2cNJZweWgc1QktL
AoZN/MeCiGVGiJZmtmyKihPMGyyLGqm6krvWFfOdqlA85+WdQyvDsevTVVp/OiEB
al4SsIvMG+U+UQaI1wIBIw==
-----END PUBLIC KEY-----

rfs7000-37FABE(config)#


rfs7000-37FABE(config)#show crypto key rsa on rfs7000-37FABE
+------------+-----------------------------------------+----------------
|     #      |                KEY NAME                 |      KEY LENGTH     |
+------------+-----------------------------------------+----------------
| 1          | default-trustpoint-srvr-priv-key        | 1024               |
| 2          | default_rsa_key                         | 1024               |
```

```
+------------+-----------------------------------------+--------------------+
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show crypto pki trustpoints all on rfs7000-37FABE

Trustpoint Name: default-trustpoint        (self signed)
-------------------------------------------------------------------------
  CRL present: no
  Server Certificate details:
    Key used: default-trustpoint-srvr-priv-key
    Serial Number: 0671
    Subject Name:
      C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EWLAN, CN=Motorola
    Issuer Name:
      C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EWLAN, CN=Motorola
    Valid From : Tue Sep 22 16:19:51 2009 UTC
    Valid Until: Wed Sep 22 16:19:51 2010 UTC


rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show crypto pki trustpoints all

Trustpoint Name: default-trustpoint        (self signed)
-------------------------------------------------------------------------
  CRL present: no
  Server Certificate details:
    Key used: default-trustpoint-srvr-priv-key
    Serial Number: 0671
    Subject Name:
      C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EWLAN, CN=Motorola
    Issuer Name:
      C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EWLAN, CN=Motorola
    Valid From : Tue Sep 22 16:19:51 2009 UTC
    Valid Until: Wed Sep 22 16:19:51 2010 UTC

rfs7000-37FABE(config)#
rfs7000-37FABE(config)#show crypto pki trustpoints
+-------------------------------+-----------------------------------------+-------
-----------------------------------+
|TRUSTPOINT         |   KEY NAME                |            VALID UNTIL              |
+-------------------------------+-----------------------------------------|default-
trustpoint|default-trustpoint-srvr-priv-key |Wed Sep 22 16:19:51 2010 UTC  |
+-------------------------------+-----------------------------------------rfs7000-
37FABE(config)#
```

6.1.14 debug

show commands

Displays debugging configuration information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show debug [profile|xpath]
show debug profile <WORD> {arg <WORD>}
show debug xpath [count|get|list]
show debug xpath [count|list] <WORD>
show debug xpath get <WORD> {option|param <WORD>} [do-profiling|
no-pretty|show-tail-only|use-streaming] {do-profiling|
no-pretty|show-tail-only|use-streaming}
```

Parameters

profile <WORD> {arg <WORD>}	Displays profile functions debugging information • <WORD> – Specify the function name • arg <WORD> – Specify arguments for the function in a single word, separated by a coma (e.g., _cli,[3,4])
xpath [count|get|list]	Displays xpath based operations debugging information • count <WORD> – Prints the number of items under an xpath node • list <WORD> – Lists the names (keys) under an xpath node • get <WORD> {option|param <WORD>} [do-profiling|no-pretty|show-tail-only|use-streaming] – Prints the value of an xpath node based on option or parameters • option – Specify options for the debug command • param <WORD> – Specify parameters for the xpath • do-profiling – Performs profiling • no-pretty – Disables pretty for speed • show-tail-only – Displays only the tail of the result • use-streaming – Uses streaming interface

Example

```
rfs7000-37FABE(config)#show debug xpath count /wing-stats
Success: 4
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show debug xpath get word option do-profiling no-pretty
Sun Dec  5 08:52:08 2010    /var/profile

         26 function calls in 0.001 CPU seconds

Ordered by: standard name
```

```
   ncalls  tottime  percall  cumtime  percall filename:lineno(function)
    1    0.000    0.000    0.001    0.001 <string>:1(<module>)
    1    0.000    0.000    0.001    0.001 cluster_db_api.py:20(cluster_db_get_api)
    1    0.000    0.000    0.001    0.001 debugcli.py:150(debug_xpath_get_stats_body)
    2    0.000    0.000    0.000    0.000 log.py:133(dlog)
    1    0.000    0.000    0.000    0.000 re.py:144(sub)
    1    0.000    0.000    0.000    0.000 re.py:227(_compile)
    1    0.000    0.000    0.000    0.000 utils.py:147(dlog_stats)
    1    0.000    0.000    0.000    0.000 utils.py:159(dlog_snmp)
    1    0.000    0.000    0.000    0.000 xpath_parser.py:104(__init__)
    1    0.000    0.000    0.000    0.000 xpath_parser.py:124(splitsegments)
    1    0.000    0.000    0.000    0.000 xpath_parser.py:194(stripFilters)
    1    0.000    0.000    0.000    0.000 xpath_parser.py:6(__init__)
    1    0.000    0.000    0.000    0.000 {built-in method sub}
    1    0.000    0.000    0.000    0.000 {isinstance}
    2    0.000    0.000    0.000    0.000 {len}
    2    0.000    0.000    0.000    0.000 {method 'append' of 'list' objects}
   1   0.000   0.000   0.000   0.000 {method 'disable' of '_lsprof.Profiler' objects}
    1    0.000    0.000    0.000    0.000 {method 'find' of 'str' objects}
    3    0.000    0.000    0.000    0.000 {method 'get' of 'dict' objects}
     2    0.000    0.000    0.000    0.000 {method 'startswith' of 'str' objects}
done profiling
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show debug xpath list /wing-stats
Success: ['cluster', 'device', 'rf_domain', 'noc']
rfs7000-37FABE(config)#
```

6.1.15 debugging

show commands

Displays debugging configuration information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show debugging {advanced-wips|captive-portal|cfgd|dhcpsvr|mstp|nsm|on|
radius|snmp|voice|vpn|wireless}
show debugging advanced-wips
show debugging {captive-portal|dhcpsvr|mstp|nsm|radius|voice|vpn|wireless} {on
<DEVICE-OR-DOMAIN-NAME>}
show debugging {on <DEVICE-OR-DOMAIN-NAME>}
```

```
show debugging snmp {on <DEVICE-NAME>}
```

Parameters

debugging {advanced-wips|captive-portal| cfgd|dhcpsvr|mstp|on|radius|voice|vpn|wireless}	Displays debugging functions:
	• captive-portal – Displays the debugging configuration of a hotspot (HSD) module
	• mstp – Displays the debugging configuration of a Multiple Spanning Tree (MST) module
	• nsm – DIsplays the debugging configuration of *Network Service Module* (NSM)
	• voice – Displays the debugging configuration of a voice module
	• wireless – Displays the debugging configuration of a wireless module
	• cfgd – Displays debugging information of a Cfgd process
	• dhcpsvr – Displays debugging information of a DHCP server configuration module
	• radius –Displays debugging information for a RADIUS configuration module
	• vpn – Displays debugging information for a VPN module
	• snmp {on <DEVICE-NAME>} – Displays the debugging configuration of SNMP module
	  • {on <DEVICE-NAME>} – On AP/Controller
	  • <DEVICE-NAME> – On AP/Controller name
	The following parameters are common for all the above except advanced-wips:
	• on – On AP/Controller or RF Domain
	  • <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF Domain name
	• advanced-wips – Displays the debugging configuration of Advanced-WIPS module

Example

```
rfs7000-37FABE(config)#show debugging mstp on rfs7000-37FABE
rfs7000-37FABE(config)#

rfs7000-37FABE(config-critical-resource-policy-test)#show debugging vpn on rfs7000-
37FABE
rfs7000-37FABE(config-critical-resource-policy-test)#

rfs7000-37FABE(config-critical-resource-policy-test)#show debugging radius on
rfs7000-37FABE
rfs7000-37FABE(config-critical-resource-policy-test)#
```

6.1.16 device-categorization

show commands

Displays device categorization details

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show device-categorization summary
```

Parameters

summary	Displays a device categorization summary

Example

```
rfs4000-22CDAA(config)#show device-categorization summary
-------------------------------------------------------------------------------
-----------------------------------------------------------------
 POLICY  #                   A/N      AP/CLIENT     MAC              SSID
-----------------------------------------------------------------------------
DEVICE-CATEGORIZATION   1   sanctioned    client  00-40-96-B0-BA-2D    -
DEVICE-CATEGORIZATION   2   neighboring   client  00-40-96-B0-BA-2A    -
DEVICE-CATEGORIZATION   3   sanctioned      ap    00-23-68-31-12-65   ASDF
-------------------------------------------------------------------------------       -
-             -         -                   -
rfs4000-22CDAA(config)#
```

6.1.17 event-history

show commands

Displays an event history

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show event-history {on <DEVICE-NAME>}
```

Parameters

{on <DEVICE-NAME>}	• on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE(config)#show event-history
 Wed Apr  7 18:16:06 2010  00-15-70-37-FA-BE  NO_COUNTRY_CODE  Country-code not set
in configuration. Radio operations disabled
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show event-history on rfs7000-37FABE
2011-01-05 08:44:30       00-15-70-37-FA-BE  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.10'
2011-01-05 08:39:30      00-15-70-37-FA-BE  SYSTEM    LOGIN             Successfully
logged in User: 'admin' with privilege 'superuser' from 'ssh'
2011-01-05 08:38:57       00-15-70-37-FA-BE  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.12'
2011-01-05 08:25:31       00-15-70-37-FA-BE  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.10'
2011-01-05 08:23:34       00-15-70-37-FA-BE  SYSTEM     LOGOUT              Logged
out User: 'admin' with privilege 'superuser' from '172.16.10.12'
2011-01-05 08:21:09      00-15-70-37-FA-BE  SYSTEM    LOGIN             Successfully
logged in User: 'admin' with privilege 'superuser' from 'ssh'
2011-01-05 08:20:42      00-15-70-37-FA-BE  SYSTEM    LOGIN             Successfully
logged in User: 'admin' with privilege 'superuser' from 'ssh'
2011-01-05 05:35:35      00-15-70-37-FA-BE  SYSTEM    LOGIN             Successfully
logged in User: 'admin' with privilege 'superuser' from 'ssh'
--------------------------------------------------------------------------------
Country of operation configured to IN [India]
rfs7000-37FABE(config)#
```

6.1.18 event-system-policy

show commands

Displays event system policy configuration information in detail

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY>
```

Parameters

[config|detail] <EVENT-SYSTEM-POLICY>	• config – Displays configuration information for the selected policy • detail – Displays configuration information for the selected policy in detail • <EVENT-SYSTEM-POLICY> – Specify the event system policy name

Example

```
rfs7000-37FABE(config)#show event-system-policy config testpolicy
--------------------------------------------------------------------------
MODULE          EVENT            SYSLOG    SNMP   FORWARD        EMAIL
--------------------------------------------------------------------------
aaa       radius-discon-msg      on        on      on         default
--------------------------------------------------------------------------
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show event-system-policy detail testpolicy
--------------------------------------------------------------------------
 MODULE                 EVENT                SYSLOG     SNMP    FORWARD    EMAIL
--------------------------------------------------------------------------
aaa      radius-discon-msg             on        on        on     default
aaa       radius-session-expired          default   default   default   default
aaa       radius-session-not-started    default   default   default   default
aaa       radius-vlan-update              default   default   default   default
adv-wips adv-wips-event-1              default   default   default     default
```

6.1.19 file

show commands

Displays file system information

NOTE: This command is not present in USER EXEC Mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show file [information <FILE>|systems]
```

Parameters

[information <FILE>|systems]	• information <FILE> – Displays file system information • <FILE> – Displays information for a specified file • systems – Displays the list of file systems present in the system

Example

```
rfs7000-37FABE(config)#show file systems
File Systems:

     Size(b)      Free(b)      Type  Prefix
           -            -    opaque  system:
    10485760      9916416     flash  nvram:
    20971520     20131840     flash  flash:
           -            -   network  (null)
           -            -   network  rdp:
           -            -   network  sftp:
           -            -   network  http:
           -            -   network  ftp:
           -            -   network  tftp:
    20971520     20131840         -  hotspot:
rfs7000-37FABE(config)#
```

6.1.20 firewall

show commands

Displays wireless firewall information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show firewall [dhcp snoop-table|dos stats|flows]{on <DEVICE-NAME>}]
show firewall flows {filter|management|on <DEVICE-NAME>|stats|wireless-client <MAC>}

show firewall flows filter {dir|dst port <1-65535>|ether[dst <MAC>|host <MAC>|src
<MAC>|vlan <1-4095>]|flow-type [bridge|natted|routed|
wired|wireless]|icmp {code|type}|igmp|ip[dst <IP>|proto <0-254>|host <IP>
{and}|src]|max-idle|min-bytes|min-pkts|not|port|src <IP> {and}|tcp|udp}
show firewall flows filter dir [wired-wired| wired-wireless|wireless-wired|wireless-
wireless] {dst|ether|flow-type|ip|max-idle|min-bytes|
min-pkts|port|src}
show wireless flows filter ether vlan <1-4095> {and|dst|ether|
flow-type|ip|max-idle|min-bytes|min-pkts|port|src|src}

show firewall flows {management|stats} {on <DEVICE-NAME>}
```

Parameters

dhcp snoop-table|dos stats|flows]{on <DEVICE-NAME>}	• dhcp snoop table – Displays DHCP snoop-table entries • dos stats – Displays a list of statistics denied from service • flows {filter|management|on <DEVICE-NAME>|stats|wireless-client <MAC>} – Displays that a session has been established • filter dir|dst port <1-65535>|ether[dst <MAC>|host <MAC>|src <MAC>|vlan <1-4095>]|flow-type [bridge|natted|routed| wired|wireless]|icmp {code|type}|igmp|ip[dst <IP>|proto <0-254> |host <IP>{and}|src]|max-idle|min-bytes|min-pkts|not|port|src<IP> {and}|tcp|udp} – Displays filter parameters • dir [wired-wired|wired-wireless|wireless-wired|wireless-wire-less] – Matches flow direction • wired-wired – Wired to wired flows • wired-wireless – Wired to wireless flows • wireless-wired – Wireless to wired flows • wireless-wireless – Wireless to wireless flows • dst – Matches only destination port • ether [dst <MAC>|host <MAC>|src <MAC>|vlan <1-4095>] – Displays ethernet parameters • dst – Matches only destination MAC address • host – Matches flows containing MAC address • src – Matches only source MAC address • vlan <1-4094> – Matches the VLAN of the traffic • flow-type [bridge|natted|routed| wired|wireless] – Matches the flow type • bridged – Bridged flows • natted – Natted flows • routed – Routed flows • wired – Flows belonging to wired hosts • wireless – Flows containing a mobile unit • icmp {code|type} – Matches flows with given ICMP code and ICMP type

	• igmp – Matches IGMP flows
	• ip [dst <IP>|proto <0-254>|host <IP> |src] – Displays IP V4 parameters
	  • dst <IP> – Matches destination IP address
	  • host <IP> – Matches flows containing IPv4 address
	  • proto <0-254> – Matches the IPv4 protocol
	  • src <IP> – Matches source IP address

	• max-idle – Matches flows which are idle at most for the given duration • min-bytes – Matches flows which has seen at least the given number of bytes • min-idle – Matches flows which are idle at least for the given duration • min-pkts – Matches flows with at least the given number of packets • not – Negates the Filter Expression • port <1-65535> – Matches either source or destination port • src port <1-65535> – Matches only source port • tcp – Matches TCP flows • udp – Matches UDP flows • management on <DEVICE-NAME> – Displays firewall flows for management traffic • stats on <DEVICE-NAME> – Displays summary of active sessions • on – On AP/Controller • <DEVICE-NAME> – On AP/Controller name • wireless-client <MAC> – Displays firewall flows for wireless clients

Example

```
rfs7000-37FABE(config)#show firewall dhcp snoop-table on rfs7000-37FABE
Snoop Binding <157.235.208.252, 00-15-70-37-FA-BE, Vlan 4>
Type Controller-SVI, Touched 32 seconds ago
------------------------------------------------------------------------
Snoop Binding <172.16.10.2, 00-15-70-37-FA-BE, Vlan 1>
Type Controller-SVI, Touched 1 seconds ago
------------------------------------------------------------------------
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show firewall dos stats on rfs7000-37FABE
+--------------------------------+-----------------+---------------------
|           ATTACK TYPE          |      COUNT      |      LAST OCCURENCE      |
+--------------------------------+-----------------+---------------------
| udp-short-hdr                  | 0               | Never                    |
| tcp-xmas-scan                  | 0               | Never                    |
| ascend                         | 0               | Never                    |
| ftp-bounce                     | 0               | Never                    |
| tcp-null-scan                  | 0               | Never                    |
| bcast-mcast-icmp               | 0               | Never                    |
| fraggle                        | 0               | Never                    |
| router-advt                    | 0               | Never                    |
| tcp-post-syn                   | 0               | Never                    |
| winnuke                        | 0               | Never                    |
| tcp-header-fragment            | 0               | Never                    |
| tcp-ip-ttl-zero                | 0               | Never                    |
| invalid-protocol               | 0               | Never                    |
| icmp-router-solicit            | 0               | Never                    |
| tcp-intercept                  | 0               | Never                    |
| twinge                         | 0               | Never                    |
| land                           | 0               | Never                    |
| spoof                          | 0               | Never                    |
```

```
| source-route                     | 0               | Never                    |
| tcp-bad-sequence                 | 0               | Never                    |
| tcp-fin-scan                     | 0               | Never                    |
| snork                            | 0               | Never                    |
| chargen                          | 0               | Never                    |
| smurf                            | 0               | Never                    |
+----------------------------------+-----------------+--------------------
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show firewall flows brief on rfs7000-37FABE
Active Flows       7
TCP flows          3
UDP flows          2
DHCP flows         0
ICMP flows         0
IPsec flows        0
L3/Unknown flows   2
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show firewall flows management on rfs7000-37FABE
========== Flow# 1 Summary ==========
Forward:
 Vlan 1, TCP 172.16.10.10 port 3995 > 172.16.10.1 port 22
 00-02-B3-28-D1-55 > 00-15-70-37-FA-BE, ingress port ge1
 Egress port: <local>, Egress interface: vlan1, Next hop: <local> (00-15-70-37-FA-BE)
 573 packets, 49202 bytes, last packet 0 seconds ago
Reverse:
 Vlan 1, TCP 172.16.10.1 port 22 > 172.16.10.10 port 3995
 00-15-70-37-FA-BE > 00-02-B3-28-D1-55, ingress port local
 Egress port: ge1, Egress interface: vlan1, Next hop: 172.16.10.10 (00-02-B3-28-D1-55)
 552 packets, 63541 bytes, last packet 0 seconds ago
TCP state: Established
Flow times out in 1 hour 30 minutes

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show firewall flows stats  on rfs7000-37FABE
Active Flows       2
TCP flows          1
UDP flows          0
DHCP flows         1
ICMP flows         0
IPsec flows        0
L3/Unknown flows   0
rfs7000-37FABE(config)#
```

6.1.21 interface

show commands

Displays the status of the different controller interfaces

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show interfaces [<WORD>|brief|counters|ge|me1|on|pc||switchport|vlan] {on <DEVICE-NAME>}
```

Parameters

interfaces [<WORD>|brief|counters|ge|me1|on|pc||Controllerport|vlan] {on <DEVICE-NAME>}	Displays the interface name • <WORD> – Displays the interface name • brief – Displays a brief summary of interface status and configuration • ge <1-4> – Displays the configured Gigabit Ethernet interface status • me1– Displays the Fast Ethernet interface status • counters – Displays interface TX/RX counters • on – Displays information on AP/controller • pc <1-4> – Displays port-channel information • Controllerport – Displays the status of layer2 interfaces • vlan <1-4094> – Displays configured vlan information The following parameters are common for the above: • on – Displays information on AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller/RF Domain name

Example

```
rfs7000-37FABE(config)#show interface Controllerport on rfs7000-37FABE
+--------------------+----------------+------------------+--------------
|     INTERFACE      |      STATUS    |        MODE      |      VLAN(S)      |
+--------------------+----------------+------------------+--------------
| ge3                | DOWN           | access           | 1                 |
| ge2                | UP             | access           | 1                 |
| ge1                | UP             | access           | 1                 |
| ge4                | DOWN           | access           | 1                 |
+--------------+----------------+------------------+------------------+
A '*' next to the VLAN ID indicates the native vlan for that trunk port
rfs7000-37FABE(config)#


rfs7000-37FABE(config)#show interface vlan 1
Interface vlan1 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 4, Metric: 1, MTU: 1500
```

```
  IP-Address: 172.16.10.2/24
    input packets 34801, bytes 5380250, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 7848, bytes 6847627, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show interface ge 2 on rfs7000-37FABE
Interface ge2 is UP
  Hardware-type: ethernet, Mode: Layer 2, Address: 00-15-70-37-FA-C0
  Index: 2002, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational 100M, Maximum 1G
  Duplex: Admin Auto, Operational Full
  Active-medium: Copper
  Controllerport settings: access, access-vlan: 1
    Input packets 6, bytes 620, dropped 0
    Received 0 broadcasts, 6 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 45524, bytes 8708231, dropped 0
    Sent 21302 broadcasts, 22261 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show interface counters
+---------+-------------------+-------+---------+----------+-------+------
|INTERFACE|MAC|RX-PKTS| RX-BYTES|RX-DROPPED|TX-PKTS|TX-BYTES|TX-DROPPED|
+---------+-------------------+-------+---------+----------+-------+------
| ge3     | 00-15-70-37-FA-C1 | 0     | 0       | 0        | 46592 | 8946900  | 0        |
| ge2     | 00-15-70-37-FA-C0 | 6     | 620     | 0        | 46582 | 8914407  | 0        |
| ge1     | 00-15-70-37-FA-BF | 56429 | 9384360 | 0        | 18047 | 12019031 | 0        |
| ge4     | 00-15-70-37-FA-C2 | 0     | 0       | 0        | 46592 | 8946900  | 0        |
| me1     | 00-15-70-CC-5E-F7 | 0     | 0       | 0        | 0     | 0        | 0        |
| vlan44  | 00-15-70-37-FA-BE | 0     | 0       | 0        | 0     | 0        | 0        |
| vlan1   | 00-15-70-37-FA-BE | 46471 | 7221803 | 0        | 9875  | 9106192  | 0        |
| vlan4   | 00-15-70-37-FA-BE | 0     | 0       | 0        | 0     | 0        | 0        |
+---------+-------------------+-------+---------+----------+-------+------
```

6.1.22 ip

show commands

Displays Internet Protocol (IP) related information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show ip [arp|ddns|dhcp|dhcp-vendor-options|domain-name|igmp|interface|name-
server|nat|route|routing]
show ip arp {<VLAN Name> {on <DEVICE-NAME>}|on <DEVICE-NAME>}

show ip ddns bindings {on <DEVICE-NAME>}

show ip dhcp [bindings|networks|status]
show  ip dhcp bindings {on <DEVICE-NAME>|manual
{on <DEVICE-NAME>}}
show ip dhcp networks {on <DEVICE-NAME>}
show  ip dhcp status {on <DEVICE-NAME>}
show ip [dhcp-vendor-options|domain-name|routing] {on <DEVICE-NAME>}
show ip igmp snooping [mrouter|vlan]
show ip igmp snooping mrouter vlan <1-4095> {on <DEVICE-NAME>}
show ip igmp snooping vlan <1-4095> {<A.B.C.D>|on}
show ip igmp snooping vlan <1-4095> {on <DEVICE-NAME>|<A.B.C.D> {on <DEVICE-NAME>}}

show ip interface {<word>|brief|on}
show ip interface <word> {on <DEVICE-NAME>}
show ip interface brief {on <DEVICE-NAME>}
show ip interface {on <DEVICE-NAME>}

show ip nat translations verbose {on <DEVICE-NAME>}

show ip route {<WORD>|ge|me1|on|pc|vlan}
show ip route <WORD> {on <DEVICE-NAME>}
show ip route ge <1-4> {on <DEVICE-NAME>}
show ip route me1 {on <DEVICE-NAME>}
show ip route {on <DEVICE-NAME>}
show ip route pc <1-4> {on <DEVICE-NAME>}
show ip route vlan <1-4094> {on <DEVICE-NAME>}
```

Parameters

arp {<VLAN Name> {on <DEVICE-NAME>}|on <DEVICE-NAME>}	Displays the ARP configuration • <WORD> – Specify the vlan name • {on <DEVICE-NAME>} – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name • {on <DEVICE-NAME>} – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name
ddns bindings {on <DEVICE-NAME>}	Displays the DDNS configuration • bindings {on <DEVICE-NAME>} – DNS address bindings • {on <DEVICE-NAME>} – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name
dhcp [bindings|networks|status] {on <DEVICE-NAME>}	Displays the DHCP server configuration • bindings {on <DEVICE-NAME>|manual {on <DEVICE-NAME>} – DNS address bindings • {on <DEVICE-NAME>} – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name • manual – Displays static DHCP address bindings • {on <DEVICE-NAME>} – Displays information on the AP/ Controller • <DEVICE-NAME> – Displays information on the AP/Controller name • networks {on <DEVICE-NAME>} – Network information • {on <DEVICE-NAME>} – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name • status {on <DEVICE-NAME>} – Displays status information • {on <DEVICE-NAME>} – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name

igmp snooping [mrouter|vlan]	Displays *Internet Group Management Protocol* (IGMP) information • snooping – IGMP snooping • mrouter vlan <1-4095> {on <DEVICE-NAME>} – Multicast router • vlan <1-4095> – Specifies a VLAN index value from 1 and 4095 • {on <DEVICE-NAME>} – Displays information on the AP/ Controller • <DEVICE-NAME>} – Displays information on the AP/ Controller name • vlan <1-4095> {on <DEVICE-NAME>|<A.B.C.D> {on <DEVICE-NAME>} – Specifies a VLAN index value from 1 and 4095 • {on <DEVICE-NAME>} – Displays information on the AP/ Controller • <DEVICE-NAME>} – Displays information on the AP/Controller name
interface {<WORD>|brief|on}	Use the show ip interface command to display the administrative and operational status of all Layer-3 interfaces or a specified Layer-3 interface. • <WORD> – Interface name • brief – Brief summary of the IP status and its configuration The following parameters are common for the above. • {on <DEVICE-NAME>} – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name • on – Displays information on AP/controller • <DEVICE-NAME>} – Displays information on the AP/Controller name

nat translations verbose {on <DEVICE-NAME>}	Displays *Network Address Translation* (NAT) information
	• translations – Displays NAT translations
	  • verbose – Displays NAT Translations in real-time
	  • on <DEVICE-NAME>} – Displays information on the AP/ Controller
	  • <DEVICE-NAME>} – Displays information on the AP/ Controller/RF Domain name

route {<WORD>|ge|me1|on|pc| vlan}	Displays route table information
	• <WORD> – Interface name
	• ge <1-4> – Displays the configured Gigabit Ethernet interface status
	• me1 – Displays the FastEthernet interface status
	• pc <1-4> – Displays information on the AP/controller
	• Controllerport – Displays the status of layer2 interfaces
	• vlan <1-4094> – Displays configured VLAN information
	The following parameters are common for the above:
	  • {on} – Displays information on AP/Controller
	  • <DEVICE-NAME> – Displays information on the AP/Controller name
	• on <DEVICE- NAME> – Displays information on the AP/Controller
	  • <DEVICE-NAME> – Displays information on the AP/Controller name

Example

```
rfs7000-37FABE(config)#show ip arp test on rfs7000-37FABE
+--------------------+-------------------------+---------------+----------
|         IP         |           MAC           |   INTERFACE   |      TYPE      |
+--------------------+-------------------------+---------------+----------------+
| 172.16.10.11       | 00-50-DA-95-11-13       | vlan1         | dynamic        |
| 172.16.10.10       | 00-02-B3-28-D1-55       | vlan1         | dynamic        |
+--------------------+-------------------------+---------------+----------
rfs7000-37FABE(config)#


rfs7000-37FABE(config)#show ip interface brief on rfs7000-37FABE
+-----------------+----------------------------+--------------+-----------
|    INTERFACE    |      IP-ADDRESS/MASK       |    STATUS    |    PROTOCOL     |
+-----------------+----------------------------+--------------+-----------
| me1             | unassigned                 | DOWN         | down            |
| vlan44          | unassigned                 | UP           | up              |
| vlan1           | 172.16.10.2/24             | UP           | up              |
| vlan4           | 157.235.208.252/24         | UP           | up              |
+-----------------+----------------------------+--------------+-----------
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip nat translations verbose on rfs7000-37FABE

PROTO ACTUAL SOURCE       ACTUAL DESTINATION   NATTED SOURCE       NATTED DESTINATION
-------------------------------------------------------------------------------

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route test on rfs7000-37FABE
+------------------------+--------------------+------------+-------------
|       DESTINATION      |      GATEWAY       |   FLAGS    |    INTERFACE     |
+------------------------+--------------------+------------+-------------
```

```
| 157.235.208.0/24        | direct              | C          | vlan4           |
| 172.16.10.0/24          | direct              | C          | vlan1           |
| default                 | 172.16.10.9         | CG         | vlan1           |
+-------------------------+---------------------+------------+-------------
Flags:  C - Connected G - Gateway
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route pc 2
+-------------------------+---------------------+------------+-------------
|       DESTINATION       |      GATEWAY        |   FLAGS    |    INTERFACE     |
+-------------------------+---------------------+------------+-------------
| 157.235.208.0/24        | direct              | C          | vlan4           |
| 172.16.10.0/24          | direct              | C          | vlan1           |
| default                 | 172.16.10.9         | CG         | vlan1           |
+-------------------------+---------------------+------------+-------------
Flags:  C - Connected G - Gateway
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route vlan 1 on rfs7000-37FABE
+-------------------------+---------------------+-------------+------------
|      DESTINATION        |       GATEWAY       |    FLAGS    |    INTERFACE    |
+-------------------------+---------------------+-------------+------------
| 172.16.10.0/24          | direct              | C           | vlan1           |
| default                 | 172.16.10.9         | CG          | vlan1           |
+-------------------------+---------------------+-------------+------------
Flags:  C - Connected G - Gateway
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip route ge 1 on rfs7000-37FABE
-------------------------------------------------------------------------------
   DESTINATION             GATEWAY          FLAGS           INTERFACE
-------------------------------------------------------------------------------
  172.16.12.0/24            direct            C              vlan3
  172.16.11.0/24            direct            C              vlan2
  172.16.10.0/24            direct            C              vlan1
-------------------------------------------------------------------------------
Flags:  C - Connected G - Gateway
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip routing on rfs7000-37FABE
IP routing is enabled.
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show ip dhcp status on rfs7000-37FABE
State of DHCP server: running
Interfaces: vlan2, vlan3
rfs7000-37FABE(config)#
```

6.1.23 ip-access-list-stats

show commands

Displays IP access list statistics

NOTE: This command is not present in the USER EXEC Mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show ip-access-list-stats {on <DEVICE-NAME>|<IP-ACCESS-LIST> {on <DEVICE-NAME>}
```

Parameters

{on <DEVICE-NAME>|<IP-ACCESS-LIST> {on <DEVICE-NAME>}	• on <DEVICE-NAME> – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the Controller name • <IP-ACCESS-LIST> – Specifies the name of the ip-access-list used to view statistics • on <DEVICE-NAME> – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name

Example

```
rfs7000-37FABE(config)#sh ip-access-list-stats
IP Access-list: # Restrict Management ACL #
  permit tcp any any eq ftp rule-precedence 1        Hitcount: 0
  permit tcp any any eq www rule-precedence 2        Hitcount: 41
  permit tcp any any eq ssh rule-precedence 3        Hitcount: 448
  permit tcp any any eq https rule-precedence 4        Hitcount: 0
  permit udp any any eq snmp rule-precedence 5       Hitcount: 0
  permit tcp any any eq telnet rule-precedence 6       Hitcount: 4
```

6.1.24 licenses

show commands

Displays installed licenses and usage information

NOTE: This command is not present in the 'Privileged Exec' mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show licenses
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show licenses
Serial Number : 6268529900014

Device Licenses:
  AP-LICENSE
    String      :
8088bb045018988b85bc05750ab7dbc802885bcc680a96194dfbeedc28d4117058eb53bd8b
    Value       : 50
    Used        : 0
  AAP-LICENSE
    String      :
8088bb045018988b5985f7127ca1d354bc689885fcc6b625b695384946d4117058eb53bd8b
    Value       : 50
    Used        : 0
rfs7000-37FABE(config)#
```

6.1.25 lldp

show commands

Displays Link Layer Discovery Protocol information on AP/Controller

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show lldp neighbors {on <DEVICE-NAME>}
```

Parameters

neighbors {on <DEVICE-NAME>}	Displays LLDP neighbor table information • on <DEVICE-NAME> – On AP/Controller • <DEVICE-NAME> – AP/Controller name

Example

```
rfs7000-37FABE(config)#show lldp neighbors
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show lldp neighbors on rfs7000-37FABE
rfs7000-37FABE(config)#
```

6.1.26 logging

show commands

Displays logging information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show logging {on <DEVICE-NAME>}
```

Parameters

logging *{on <DEVICE-NAME>}*	Displays logging information on an AP or controller

Example

```
rfs7000-37FABE(config)#show logging ?
  on  On AP/Controller
  |   Output modifiers
  >   Output redirection
  >>  Output redirection appending
  <cr>

rfs7000-37FABE(config)#show logging on ?
  DEVICE-NAME  AP / Controller name

rfs7000-37FABE(config)#show logging on rfs7000-37FABE

Logging module: enabled
    Aggregation time: disabled
    Console logging: level warnings
    Monitor logging: disabled
    Buffered logging: level warnings
    Syslog logging: level warnings
        Facility: local7

Log Buffer (18226 bytes):


Jan 27 18:04:54 2010: %CERTMGR-4-CERT_EXPIRY: server certificate for trustpoint
mint_security_trustpoint has expired
Jan 27 18:04:54 2010: %CERTMGR-4-CERT_EXPIRY: ca certificate for trustpoint
mint_security_trustpoint has expired
Jan 27 17:04:54 2010: %CERTMGR-4-CERT_EXPIRY: server certificate for trustpoint
mint_security_trustpoint has expired
Jan 27 17:04:54 2010: %CERTMGR-4-CERT_EXPIRY: ca certificate for trustpoint
mint_security_trustpoint has expired
Jan 27 16:04:54 2010: %CERTMGR-4-CERT_EXPIRY: server certificate for trustpoint
mint_security_trustpoint has expired
Jan 27 16:04:54 2010: %CERTMGR-4-CERT_EXPIRY: ca certificate for trustpoint
mint.....................................................
rfs7000-37FABE(config)#
```

6.1.27 mac-access-list-stats

show commands

Displays MAC-access list statistics

NOTE: This command is not present in USER EXEC Mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show mac-access-list-stats {on <DEVICE-NAME>|<IP-ACCESS-LIST> {on <DEVICE-NAME>}}
```

Parameters

{on <DEVICE-NAME>| <MAC-ACCESS-LIST> {on <DEVICE-NAME>}	• on <DEVICE-NAME> – Displays information on the AP/Controller
	  • <DEVICE-NAME> – Displays the AP/Controller name
	• <MAC-ACCESS-LIST> – Specifies the name of the MAC-access-list used to view statistics
	  • on <DEVICE-NAME> – Displays information on the AP/Controller
	  • <DEVICE-NAME> – Displays the AP/Controller name

Example

```
rfs7000-37FABE(config)#show mac-access-list-stats on rfs7000-37FABE
rfs7000-37FABE(config)#
```

6.1.28 mac-address-table

show commands

Displays MAC address table entries

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show mac-address-table {on <DEVICE-NAME>}
```

Parameters

{on <DEVICE-NAME>}	• on <DEVICE-NAME> – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name

Example

```
rfs7000-37FABE(config)#show mac-address-table on rfs7000-37FABE
+------------+----------+-----------+--------------------------+-----------
|   BRIDGE   |   VLAN   |    PORT   |           MAC            |    FORWARD     |
+------------+----------+-----------+--------------------------+-----------
| 1          | 1        | ge1       | 00-50-DA-EE-B5-5C        | forward        |
| 1          | 1        | ge1       | 00-A0-F8-00-00-00        | forward        |
| 1          | 1        | ge1       | 00-02-B3-28-D1-55        | forward        |
| 1          | 1        | ge1       | 00-A0-F8-68-D5-5D        | forward        |
| 1          | 1        | ge1       | 00-50-DA-95-11-13        | forward        |
| 1          | 1        | ge1       | 00-15-70-38-06-53        | forward        |
| 1          | 1        | ge1       | 00-15-70-41-9F-7F        | forward        |
| 1          | 1        | ge1       | 00-15-70-88-9E-C4        | forward        |
+------------+----------+-----------+--------------------------+-----------
rfs7000-37FABE(config)#
```

6.1.29 mint

show commands

Displays MiNT protocol configuration commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show mint [dis|id|known-adopters|links|lsp|lsp-db|mlcp|neighbors
|route|security|stats]
show mint [dis {on <DEVICE-NAME>|links {detail on <DEVICE-NAME>|on <DEVICE-
NAME>}|lsp|lsp-db {detail on <DEVICE-NAME>|on <DEVICE-NAME>}|mlcp {history on
<DEVICE-NAME> |on <DEVICE-NAME>}|neighbors {details on <DEVICE-NAME>|on <DEVICE-
NAME>}|security pending-approvals]

show mint [detail|known-adopters|route|stats]{on <DEVICE-NAME>}
```

Parameters

mint [dis|id|known-adopters|links detail |lsp| lsp-db|mlcp history |neighbors|route| security pending-approvals|stats]	• dis – Displays MiNT network DISes
	• id – Displays the local MiNT ID
	• known-adopters – Displays known possible, reachable adopters
	• security pending-approvals – Displays MiNT security parameters
	  • pending-approvals – Displays pending requests to join the MiNT security domain
	• links detail – Displays MiNT networking links details
	• lsp – Displays the router's MiNT LSPs
	• lsp-db details <AA.BB.CC.DD> – Displays MiNT LSP database details
	  • <AA.BB.CC.DD> – Specify the MiNT address in <AA.BB.CC.DD> format
	• mlcp history – Displays MiNT link creation protocol status
	• neighbors detail – Displays adjacent MiNT peers details
	• route – Displays MiNT route table details
	• stats – Displays MiNT related statistics
	The following is common for the above:
	• {on <DEVICE-NAME>} – On AP/Controller
	  • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE(config)#show mint stats
0 L1 neighbors
L1 LSP DB size 1 LSPs (0 KB)
1 L1 routes
Last SPFs took 0s
SPF (re)calculated 1 times.
levels 1
base priority 180
dis priority 180
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show mint lsp
id 70.37.fa.be, level 1, seqnum 18640, 0 adjacencies, 0 extended-vlans,
expires in 1145 seconds, republish in 722 seconds, changed True,
ext-vlan FDB pri 0, 180 bytes

rfs7000-37FABE(config)#show mint lsp-db
Level 1 LSPs
  70.37.fa.be: seqnum 18640, 0 adjacencies, 0 extended-vlans, expires in 1138 seconds
1 LSPs in level 1 database

rfs7000-37FABE(config)#show mint route
Destination : Next-Hop(s)
70.37.fa.be :  70.37.FA.BE
00.00.00.00 :  00.00.00.00
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show mint known-adopters on rfs7000-37FABE
70.37.FA.BE
rfs7000-37FABE(config)#
```

6.1.30 noc

show commands

Displays NOC level information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131
- AP650
- AP6511
- AP6532

Syntax

```
show noc [client-list|device|domain [managers|statistics details]]
show noc device filter {offline|online|rf-domain [RF-DOMAIN|not RF-DOMAIN] }]
```

Parameters

[client-list|device|domain [managers|statistics]]	• client-list – Displays a list of clients at the NOC level
	• device filter {offline|online|rf-domain [RF-DOMAIN|not RF-DOMAIN] – Displays device information for all devices in the network
	  • filter {offline|online|rf-domain [RF-DOMAIN|not RF-DOMAIN]} – Specifies the additional selection filter in getting table values
	  • offline – Displays devices that are offline
	  • online – Displays device that are online
	  • rf-domain [RF-DOMAIN|not RF-DOMAIN]– Displays devices on a given RF Domain
	  • RF-DOMAIN – Specify RF Domain name
	  • not – Inverts match selection
	• domain [managers|statistics] – Displays RF Domain wide information
	  • managers – Displays list of RF Domains and managers
	  • statistics details – Displays statistical information regarding RF Domains in detail

Example

```
rfs7000-37FABE(config)#show noc device
+-----------------+----------------+--------+----------------+-----------
|  MAC|  HOST-NAME  | TYPE| CLUSTER| RF-DOMAIN |ADOPTED-BY|    ONLINE  |
+-----------------+----------------+--------+----------------+-----------
|99-88-77-66-55-44|   ap7131-665544|  ap7131|    | default|     | offline    |
|00-15-70-88-9E-C4|   ap7131-889EC4|  ap7131|   | default|     | offline    |
|11-22-33-44-55-66|    ap650-445566|   ap650| |   default|     | offline    |
|00-15-70-37-FA-BE|  rfs7000-37FABE| rfs7000|    |  default|   |  online    |
+-----------------+----------------+--------+----------------+-----------
Total number of clients displayed: 4
rfs7000-37FABE(config)#
rfs7000-37FABE(config)#show noc domain statistics details
================================================================================
======
RF-Domain RFDOMAIN_UseCase1
Note: TX = AP->Client, RX = Client->AP
--------------------------------------------------------------------------------
------
Data bytes            : ( TX + RX = Total ),  0 + 0 = 0  bytes
```

```
Data throughput       : ( TX + RX = Total ),  0 Kbps + 0 Kbps = 0 Kbps
Data packets          : ( TX + RX = Total ),  0 + 0 = 0 pkts
Data pkts/sec         : ( TX + RX = Total ),  0 + 0 = 0 pps
BCMC Packets          : ( TX + RX = Total ),  0 + 0 = 0 pkts
Management Packets    : ( TX + RX = Total ),  0 + 0 = 0 pkts
Packets Discarded     : 0 - Tx Dropped, 0 - Rx Errors
Indicators            : T = 0 @ Max user rate of 0 Kbps
Distribution          : 0 Clients, 0 radios
Client count Detais   : 0/0/0 (b/bg/bgn); 0/0 (a/an)
Stats Update Info     : 6 seconds - update interval, mode is auto
Threat Level          : 0
Cause of concern      :
Remedy                :
Last update           : 2010-01-31 10:30:22 by 00-15-70-37-FA-BE
------------------------------------------------------------------------------
------

Total number of RF-domain displayed: 1
rfs7000-37FABE(config-rf-domain-RFDOMAIN_UseCase1)#

rfs7000-37FABE(config)#show noc device filter online
------------------------------------------------------------------------
MAC    HOST-NAME     TYPE        CLUSTER      RF-DOMAIN       ADOPTED-BY     ONLINE
------------------------------------------------------------------------ 00-15-70-
37-FA-BE rfs7000-37FABE rfs7000  RFDOMAI..echPubs             online
------------------------------------------------------------------------Total
number of clients displayed: 1
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show noc domain statistics details
========================================================================RF-Domain
RFDOMAIN_TechPubs
Note: TX = AP->Client, RX = Client->AP
------------------------------------------------------------------------
Data bytes            : ( TX + RX = Total ),  0 + 0 = 0  bytes
Data throughput       : ( TX + RX = Total ),  0 Kbps + 0 Kbps = 0 Kbps
Data packets          : ( TX + RX = Total ),  0 + 0 = 0 pkts
Data pkts/sec         : ( TX + RX = Total ),  0 + 0 = 0 pps
BCMC Packets          : ( TX + RX = Total ),  0 + 0 = 0 pkts
Management Packets    : ( TX + RX = Total ),  0 + 0 = 0 pkts
Packets Discarded     : 0 - Tx Dropped, 0 - Rx Errors
Indicators            : T = 0 @ Max user rate of 0 Kbps
Distribution          : 0 Clients, 0 radios
Client count Detais   : 0/0/0 (b/bg/bgn); 0/0 (a/an)
Stats Update Info     : 6 seconds - update interval, mode is auto
Threat Level          : 1
Cause of concern      : no sensors enabled in RF-domain RFDOMAIN_TechPubs
Remedy                : enable AP detection
Last update           : 2011-01-09 08:44:15 by 00-15-70-37-FA-BE
------------------------------------------------------------------------

Total number of RF-domain displayed: 1
rfs7000-37FABE(config)#
```

6.1.31 ntp

show commands

Displays *Network Time Protocol* (NTP) information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show ntp [associations {detail}|status] {on <DEVICE-NAME>}
```

Parameters

ntp [associations detail|status] {on <DEVICE-NAME>}	Displays the *Network Time Protocol* (NTP) configuration
	• associations detail – Displays existing NTP associations
	  • detail {on <DEVICE-NAME>} – Displays NTP association details
	• status {on <DEVICE-NAME>} – Displays NTP status
	  • on – On AP/Controller
	  • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE>show ntp associations
 address      ref clock     st when poll reach delay offset  disp
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
rfs7000-37FABE>

rfs7000-37FABE>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is 2**0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec
rfs7000-37FABE>

rfs7000-37FABE>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is 2^0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
rfs7000-37FABE>
```

6.1.32 password-encryption

show commands

Displays password encryption status information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show password-encryption status
```

Parameters

password-encryption status	Displays password encryption status information

Example

```
rfs7000-37FABE(config)#show password-encryption status
Password encryption is disabled
rfs7000-37FABE(config)#
```

6.1.33 power

show commands

Displays *power over ethernet* (PoE) information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
power [configuration|status] {on <DEVICE-NAME>}
```

Parameters

[configuration|status] {on <DEVICE-NAME>}	• configuration – Displays the PoE configuration • status – Displays the PoE status The following are common for the above: • on <DEVICE-NAME> – Displays information on the AP/Controller • <DEVICE-NAME> – Displays information on the AP/Controller name

Example

```
rfs6000-37FAAA(config)#show power status on rfs6000-37FAAA
System Voltage: 53.4 volts
  Guard Band: 32 watts
  Power Budget: 190 watts Power Consumption: 0 watts
  poe device 1 temperature 35C
  poe device 2 temperature 38C

--------------------------------------------------------------------------------
     PORT        VOLTS           mA          WATTS        CLASS       STATUS
--------------------------------------------------------------------------------
  ge1           0.0             0           0.0          0           Off
  ge2           0.0             0           0.0          0           Off
  ge3           0.0             0           0.0          0           Off
  ge4           0.0             0           0.0          0           Off
  ge5           0.0             0           0.0          0           Off
  ge6           0.0             0           0.0          0           Off
  ge7           0.0             0           0.0          0           Off
  ge8           0.0             0           0.0          0           Off
--------------------------------------------------------------------------------
rfs6000-37FAAA(config)#show power configuration
--------------------------------------------------------------------------------
       PORT             PRIORITY           POWER LIMIT            ENABLED
--------------------------------------------------------------------------------
  ge1              low                 30.0W                  yes
  ge2              low                 30.0W                  yes
  ge3              low                 30.0W                  yes
  ge4              low                 30.0W                  yes
  ge5              low                 30.0W                  yes
  ge6              low                 30.0W                  yes
  ge7              low                 30.0W                  yes
  ge8              low                 30.0W                  yes
--------------------------------------------------------------------------------
```

6.1.34 remote-debug

show commands

Displays remote debug session information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show remote-debugging
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show remote-debug
live-pktcap
 Not running
wireless
 Not running
copy-crashinfo
 Not running
offline-pktcap
 Not running
copy-techsupport
 Not running
more
 Not running
rfs7000-37FABE(config)#
```

6.1.35 rf-domain-manager

show commands

Displays RF Domain Manager selection details.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show rf-domain-manager
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show rf-domain-manager
 RF Domain default
 RF Domain Manager:
    ID: 70.37.fa.be
    Priority: 9
    Has IP connectivity
    Has non-mesh links
    Last change 12265 seconds ago
 This device:
    Priority: 9
    Has IP connectivity
    Has non-mesh links
rfs7000-37FABE(config)#
```

6.1.36 role

show commands

Displays role based firewall information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show role wireless-clients {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

wireless-clients {on <DEVICE-OR-DOMAIN-NAME>}	Mobile units associated with roles • on <DEVICE-OR-DOMAIN NAME> – Displays information on the AP/Controller or RF Domain • <DEVICE-OR-DOMAIN NAME> – Displays information on the AP/Controller/RF Domain name

Example

```
rfs7000-37FABE(config)#show role wireless-clients on rfs7000-37FABE
No ROLE statistics found.
rfs7000-37FABE(config)#
```

6.1.37 running-config

show commands

Displays the contents of those configuration files where all configured MAC and IP access lists are applied to an interface

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show running-config {device|include-factory|interface|wlan}
show running-config device [DEVICE|self] {include-factory}
show running-config interface {<WORD>|ge<1-4>|include-factory|me1|pc|vlan}
show running-config interface {<WORD>|ge <1-4>|me1|port-channel <1-4>|vlan <1-4094>}
{include-factory}
show running-config wlan <WLAN> {include-factory}
```

Parameters

device [DEVICE|self] {include-factory}	Displays device configuration • DEVICE – Specifies a device MAC address to view detailed information • self – Displays the currently logged device • include-factory – Includes factory defaults
include-factory	Includes default factory settings
interface {<WORD>|ge <1-4>|me1|pc <1-4>|vlan <1-4094>} {include-factory}	Displays configuration for configured interface • <WORD> – Specifies the interface name • ge <1-4> – Gigabit Ethernet interface from 1- 4include-factory – Includes factory defaults • me1 – Fast Ethernet interface • port-channel <1-4> – Port-Channel interface from 1- 4 • vlan <1-4094> – Specifies a VLAN index value from 1- 4094 The following parameter is common for all the above: • include-factory – Includes factory defaults
wlan <WLAN> {include-factory}	Displays configuration for a specific WLAN • <WLAN> {include-factory} – Specifies the name of the WLAN • include-factory – Includes factory defaults

Example

```
rfs7000-37FABE(config)#show running-config device self
!
firewall ratelimit-trust policy default
!
management-policy default
 telnet
 http server
```

```
 ssh
!
firewall-policy default
!
mint-security-policy the_policy
 rejoin-timeout 35
!
device-discover-policy default
!
rfs7000 00-15-70-37-FA-BE
 hostname rfs7000-37FABE
 no country-code
 bridge vlan 3
 bridge vlan 5
  ip arp trust
  ip dhcp trust
  ip igmp snooping querier version 2
  ip igmp snooping querier max-response-time 3
  ip igmp snooping querier timer expiry 89
 wep-shared-key-auth
 radius nas-identifier
test.....................................................................
rfs7000-37FABE(config)

rfs7000-37FABE(config)#show running-config device 11-22-33-44-55-66 include-factory
!
radio-qos-policy default
 wmm best-effort txop-limit 0
 wmm best-effort aifsn 3
 wmm best-effort cw-min 4
 wmm best-effort cw-max 6
 wmm background txop-limit 0
 wmm background aifsn 7
 wmm background cw-min 4
 wmm background cw-max 10
 wmm video txop-limit 94
 wmm video aifsn 1
 wmm video cw-min 3
 wmm video cw-max 4
 wmm voice txop-limit 47
 wmm voice aifsn 1
 wmm voice cw-min
2.....................................................................
rfs7000-37FABE(config)#
```

6.1.38 session-changes

show commands

Displays the configuration changes made in this session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show session-changes
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show session-changes

No changes in this session

rfs7000-37FABE(config)#
```

6.1.39 session-config

show commands

Displays the list of active open sessions on a device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show session-config {include-factory}
```

Parameters

session-config {include-factory}	Displays the contents of the current configuration • {include-factory} – Includes factory defaults

Example

```
rfs7000-37FABE(config)#show session-config
!
! Configuration of RFS7000 version 5.1.0.0-072R
!
!
version 2.1
!
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
igmp-snoop-policy default
 no igmp-snooping
 no querier
 unknown-multicast-fwd
!
!
mint-policy global-default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
.....
.....
.....
.....
rfs7000-37FABE(config)#
```

6.1.40 sessions

show commands

Displays CLI sessions

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show sessions {on <DEVICE-NAME>}
```

Parameters

sessions {on <DEVICE-NAME>}	Displays CLI sessions on the device • on <DEVICE-NAME> – Displays information on the AP/Controller • <DEVICE- NAME> – Displays information on the AP/Controller name

Example

```
rfs7000-37FABE(config)#show sessions
INDEX   COOKIE  NAME            START TIME              FROM
1       4       admin           Jun 16 13:05:36 2010    127.0.0.1
2       5       admin           Jun 16 13:06:19 2010    172.16.10.10
rfs7000-37FABE(config)#
```

6.1.41 smart-rf

show commands

Displays Smart RF Management commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show smart-rf [calibration-status|channel-distribution|history|
radio|interactive-calibration-config]
show smart-rf [calibration-status|channel-distribution|history|
interactive-calibration-config] {on <DOMAIN-NAME>}]
show smart-rf radio {<AA-BB-CC-DD-EE-FF>|activity|all-11an|
all-11bgn|energy|neighbors|on {<DOMAIN-NAME>}
show smart-rf radio {AA-BB-CC-DD-EE-FF>|all-11an|all-11bgn} {on
<DOMAIN-NAME>}
show smart-rf radio energy {<AA-BB-CC-DD-EE-FF>|all-11an|all-11bgn} {on <DOMAIN-
NAME>}
show smart-rf radio neighbors {<AA-BB-CC-DD-EE-FF>|all-11an|all-11bgn} {on <DOMAIN-
NAME>}]
```

Parameters

calibration-status {on <DOMAIN-NAME>}	Displays smart-rf calibration status • on <DOMAIN NAME> – Displays information on a RF Domain • <DOMAIN NAME> – Displays information on a RF Domain name
channel-distribution {on <DOMAIN-NAME>}	Display smart-rf channel distribution • on <DOMAIN NAME> – Displays information on a RF Domain • <DOMAIN NAME> – Displays information on a RF Domain name
history {on <DOMAIN-NAME>}	Displays smart-rf history • on <DOMAIN NAME> – Displays information on a RF Domain • <DOMAIN NAME> – Displays information on a RF Domain name

radio {<AA-BB-CC-DD-EE-FF>| activity|all-11an| all-11bgn|energy| neighbors|on <DOMAIN-NAME>}	Displays radio related commands
	• energy – All 11a radios currently in the configuration
	• neighbors – All 11a radios currently in the configuration
	  • <AA-BB-CC-DD-EE-FF> – Radio MAC address in <AA-BB-CC-DD-EE-FF> format (for all radios)
	  • activity – Displays number of power/channel /coverage hole related changes
	  • all-11an – All 11bg radios currently in the configuration
	  • all-11bgn – Displays radio energy
	The following are common for all the above:
	  • on <DOMAIN NAME> – Displays information on a RF Domain
	  • <DOMAIN NAME> – Displays information on a RF Domain name
	• on <DOMAIN NAME> – Displays information on a RF Domain

interactive-calibration-config {on <DOMAIN-NAME>}	Displays simulated calibration configuration • on <-DOMAIN NAME> – Displays information on a RF Domain • <DOMAIN NAME> – Displays information on a RF Domain name

Example

```
rfs7000-37FABE(config)#show smart-rf calibration-status
No calibration currently in progress
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show smart-rf history
rfs7000-37FABE(config)#
```

6.1.42 spanning-tree

show commands

Displays spanning tree information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show spanning-tree mst {configuration|detail|instance|on}
show spanning-tree mst {on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst configuration {on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst detail {interface|on}
show spanning-tree mst detail interface {<WORD>|ge<1-4>|me1|port-channel<1-4>|vlan
<1-4094>} {on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst detail {on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst instance <1-15> {interface|on}
show spanning-tree mst instance <1-15> interface <WORD>
{on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst instance {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

mst	Displays Multiple Spanning Tree (MST) information
configuration {on <DEVICE-OR-DOMAIN-NAME>}	• configuration – Displays configuration information • {on <DEVICE-OR-DOMAIN NAME>} – Displays information on the AP/Controller • <DEVICE-OR-DOMAIN NAME> – Displays information on the AP/Controller/RF Domain name
detail {interface|on}	Displays detailed information • interface – Interface information • <WORD> – Interface name • ge <1-4> – Gigabit Ethernet interface from 1-4 • me1 – Fast Ethernet interface • port-channel <1-4> – Port Channel interface • vlan <1-4094> – Select a value from 1 -4094 to set VLAN index The following parameters are common for interface commands • {on <DEVICE-OR-DOMAIN NAME>} – Displays information on the AP/Controller • <DEVICE-OR-DOMAIN NAME> – Displays information on the AP/Controller/RF Domain name • {on <DEVICE-OR-DOMAIN-NAME>} – Displays information on the AP/Controller • <DEVICE-OR-DOMAIN NAME> – Displays information on the AP/Controller/RF Domain name
instance <1-15> {interface|on}	Displays instance information • <1-15> – Select an instance ID from 1-15 • interface <WORD> {on <DEVICE-OR-DOMAIN-NAME>} – Interface information • <WORD> {on <DEVICE-OR-DOMAIN-NAME>} – Specifies the interface name • {on <DEVICE-OR-DOMAIN-NAME>} – Displays information on the AP/Controller • <DEVICE-OR-DOMAIN NAME> – Displays information on the AP/Controller/RF Domain name
{on <DEVICE-OR-DOMAIN-NAME>}	• {on <DEVICE-OR-DOMAIN-NAME>} – Displays information on the AP/Controller • <DEVICE-OR-DOMAIN NAME> – Displays information on the AP/Controller/RF Domain name

Example

```
rfs7000-37FABE(config)#show spanning-tree mst configuration on rfs7000-37FABE
%%
%  MSTP Configuration Information for bridge 1 :
%%------------------------------------------------------
%  Format Id       : 0
%  Name            : My Name
%  Revision Level  : 0
%  Digest          : 0xac36177f50283cd4b83821d8ab26de62
%%------------------------------------------------------

rfs7000-37FABE(config)#
```

```
rfs7000-37FABE(config)#show spanning-tree mst detail interface test on rfs7000-37FABE
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0  - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show spanning-tree mst detail
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0  - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off

%   ge4: Port 2004 - Id 87d4 - Role Disabled - State Forwarding
%   ge4: Designated External Path Cost 0 - Internal Path Cost 0
%   ge4: Configured  Path Cost 11520 - Add type Implicit - ref count 1
%   ge4: Designated Port Id 0 - CST Priority 128
%   ge4: ge4: CIST Root 0000000000000000
%   ge4: ge4: Regional Root 0000000000000000
%   ge4: ge4: Designated Bridge 0000000000000000
%   ge4: Message Age 0 - Max Age 0
%   ge4: CIST Hello Time 0 - Forward Delay 0
%   ge4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge4: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   ge4: Portfast configured - Current portfast on
%   ge4: portfast bpdu-guard  enabled  - Current portfast bpdu-guard off
%   ge4: portfast bpdu-filter  enabled  - Current portfast bpdu-filter off
%   ge4: no root guard configured  - Current root guard off
%   ge4: Configured Link Type point-to-point - Current point-to-point

%   ge3: Port 2003 - Id 87d3 - Role Disabled - State Forwarding
%   ge3: Designated External Path Cost 0 - Internal Path Cost 0
%   ge3: Configured  Path Cost 11520 - Add type Implicit - ref count 1
%   ge3: Designated Port Id 0 - CST Priority
128.....................................................................
.............
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show spanning-tree mst instance 1 interface test on rfs7000-
37FABE
rfs7000-37FABE(config)#
```

6.1.43 startup-config

show commands

Displays the complete startup configuration script on the console

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show startup-config {include-factory}
```

Parameters

startup-config {include-factory}	Displays the contents of the startup configuration • include-factory – Includes factory defaults

Example

```
rfs7000-37FABE(config)#show startup-config include-factory
!
! Configuration of RFS7000 version 5.1.0.0-072R
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 enable
 calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
 voice-prioritization
 svp-prioritization
 wmm background cw-max 8
 wmm video txop-limit 9
 wmm voice cw-min 6
 wmm voice cw-max 6
 rate-limit client to-air max-burst-size 3
 rate-limit client to-air red-threshold video 101
 rate-limit client from-air rate 55
 rate-limit client from-air red-
.....................................................................................
...
rfs7000-37FABE(config)#
```

6.1.44 terminal

show commands

Displays terminal configuration parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show terminal
```

Parameters

None

Example

```
rfs7000-37FABE(config)#show terminal
Terminal Type: xterm
Length: 45     Width: 126
rfs7000-37FABE(config)#
```

6.1.45 timezone

show commands

Displays the timezone of the AP or controller on the command prompt

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show timezone
```

Parameters

timezone	Displays the timezone

Example

```
rfs7000-37FABE(config)#show timezone
Timezone is America/Los_Angeles
```

6.1.46 upgrade-status

show commands

Displays the status of the last image upgrade

NOTE: This command is not present in the USER EXEC Mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show upgrade-status {detail {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

Parameters

upgrade-status {detail {on <DEVICE-NAME>}|on <DEVICE-NAME>}	Displays the last image-upgrade status
	• detail – Displays last image upgrade log
	  • on <DEVICE-NAME> – On AP/Controller
	  • <DEVICE-NAME> – On AP/Controller name
	• {on <DEVICE-NAME>} – On AP/Controller
	  • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE(config)#show upgrade-status detail on rfs7000-37FABE
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 04:12:2010 08:44:00 UTC
-------------------------------------------------------
Running from partition /dev/mtdblock6, partition to update is /dev/mtdblock7
var2 is 6 percent full
/tmp is 6 percent full
Free Memory 155900 kB
FWU invoked via Linux shell
Validating image file header
Making file system
Extracting files (this can take some time).
Version of firmware update file is 5.1.0.0-072R
Successful
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show upgrade-status on rfs7000-37FABE
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 04:12:2010 08:44:00 UTC
rfs7000-37FABE(config)#
```

6.1.47 version

show commands

Displays a device's software and hardware version

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show version {on <DEVICE-NAME>}
```

Parameters

version {on <DEVICE-NAME>	Displays the software and hardware version on a device • {on <DEVICE-NAME>} – On AP/Controller • <DEVICE-NAME> – On AP/Controller name

Example

```
rfs7000-37FABE(config)#show version on rfs7000-37FABE
RFS7000 version 5.1.0.0-072R
Copyright (c) 2006-2011 Motorola Solutions, Inc.
Booted from primary

RFS7000 uptime is 0 days, 04 hours 39 minutes
CPU is RMI XLR V0.4
255464 kB of on-board RAM
Base ethernet MAC address is 00-15-70-37-FA-BE
System serial number is 6268529900014
Model number is None
FPGA version is 3.41
rfs7000-37FABE(config)#
```

6.1.48 wireless

show commands

Displays wireless configuration parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show wireless [ap|client|domain|mesh||radio|regulatory|sensor-server|
unsanctioned|wips|wlan]
show wireless ap {configured|detail|load-balancing|on}
show wireless ap detail {on <DEVICE-OR-DOMAIN-NAME>|<DEVICE-NAME> on <DEVICE-OR-
DOMAIN-NAME>}
show wireless ap load-balancing {on <DEVICE-NAME>}
show wireless ap on <DEVICE-OR-DOMAIN-NAME>
show wireless client {detail <AA-BB-CC-DD-EE-FF> on <DEVICE-OR-DOMAIN-NAME>|filter|on
<DEVICE-OR-DOMAIN-NAME> |statistics|tspec
<AA-BB-CC-DD-EE-FF>}
show wireless client filter [ip|state|wlan]
show wireless client statistics {detail <AA-BB-CC-DD-EE-FF>|on <DEVICE-OR-DOMAIN-
NAME>}|rf|traffic|window-data}
show wireless client statistics {rf|traffic} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client window-data [<AA-BB-CC-DD-EE-FF> <1-2>|<WORD>]
show wireless client filter ip [<A.B.C.D>|not <A.B.C.D>]
show wireless client filter state [date-ready|not [data-ready|roaming]
|roaming]
show wireless client filter wlan [<WLAN>|not <WLAN>]
show wireless mesh links {on <DEVICE-OR-DOMAIN-NAME>}


show wireless  radio {detail|on|statistics|tspec}
show wireless radio [detail|tspec] [<AA-BB-CC-DD-EE-FF><1-3>|<WORD>]
show wireless radio {on <DEVICE-OR-DOMAIN-NAME>}
show wireless radio statistics {detail|on|rf|traffic|windows-data}
show wireless radio statistics { on <DEVICE-OR-DOMAIN-NAME> |rf {on
<DEVICE-OR-DOMAIN-NAME>}|traffic {on <DEVICE-OR-DOMAIN-NAME>}}
show wireless radio statistics {detail|window-data} {<AA-BB-CC-DD-EE-FF>
<1-3>|<WORD>}
show wireless regulatory [channel-info <WORD>|country-code <WORD>|
device-type]
show wireless regulatory device-type [ap650|ap7131|rfs4000] <WORD>
show wireless sensor-server  {on <DEVICE-OR-DOMAIN-NAME>}
show wireless sanctioned aps {detail|statistics|on}
show wireless sanctioned aps {detail|statistics} {on
 <DEVICE-OR-DOMAIN-NAME>}
show wireless sanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}

show wireless wips [event-history|client-blacklist]{on <DEVICE-OR-DOMAIN-NAME>}
show wireless wlan {config|detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|
policy-mappings|statistics|usage-mappings}
show wireless wlan statistics {<WLAN>|detail|on|traffic}
show wireless wlan statitics {<WLAN>|detail|traffic} {on
<DEVICE-OR-DOMAIN-NAME>}
show wireless wlan statistics  {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

ap {configured|detail |load-balancing|on}	Displays information regarding managed access points • configured – Displays information all access points in configuration • detail {on <DEVICE-OR-DOMAIN-NAME>|<DEVICE-NAME> on <DEVICE-OR-DOMAIN-NAME>} – Displays detailed information for given AP • <DEVICE-NAME> – Specify AP MAC address or its hostname • load-balancing {on <DEVICE-NAME>} – Displays load balancing status on the specified device • on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF Domain • on – On AP/Controller or RF Domain • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/RF Domain name
client {detail <AA-BB-CC-DD-EE-FF>|filter|on <DEVICE-OR-DOMAIN-NAME>| |statistics|tspec <AA-BB-CC-DD-EE-FF>}	Displays information about clients • detail <AA-BB-CC-DD-EE-FF> – Displays detailed information about a client • <AA-BB-CC-DD-EE-FF> – Specify the MAC address of the client • filter [ip|state|wlan] – Specifies an additional selection filter for getting table values • ip [<A.B.C.D>|not] – Selection by IP address • <A.B.C.D> – Specifies the IP address • not – Invert match selection • state [date-ready|not [data-ready|roaming]|roaming] – Selection based on state • data-ready – Clients in data-ready • not [data-ready|roaming] – Invert match selection • roaming – Roaming clients • wlan – Displays clients on given WLAN • WLAN – Specifies the WLAN name • not – Invert match selection • on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF Domain • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF Domain name • statistics {detail <AA-BB-CC-DD-EE-FF>|on <DEVICE-OR-DOMAIN-NAME>|rf|traffic|window-data} – Displays statistical information for clients • detail <AA-BB-CC-DD-EE-FF> – Displays detailed information about a client • <AA-BB-CC-DD-EE-FF> – Enter the MAC address of a client • rf on <DEVICE-OR-DOMAIN-NAME> – Displays information about RF related statistics • traffic on <DEVICE-OR-DOMAIN-NAME> – Displays information about data traffic related statistics

	• on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF Domain
	  • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF Domain name
	• window-data [<AA-BB-CC-DD-EE-FF> <1-2>|<WORD>] – Displays window statistics
	  • <AA-BB-CC-DD-EE-FF> <1-2> – Specifies the MAC address of the client
	  • <1-2> – Enter a numerical window number
	  • <WORD> – Enter the client window-stats id in the form of MAC followed by window number: e.g. AA-BB-CC-DD-EE-FF:W1
	• tspec <AA-BB-CC-DD-EE-FF> – Displays detailed TSPEC information for clients
	  • <AA-BB-CC-DD-EE-FF> – Specifies the MAC address of the client
	• wlan [WLAN|not] – Displays client information for a given WLAN
	  • <WLAN> – Specifies the WLAN name
	  • not <WLAN> – Invert match selection
	  • <WLAN> – Specifies the WLAN name

mesh links {on <DEVICE-OR-DOMAIN-NAME>}	Displays information on radio mesh
	• links – Displays information on the active links of the radio mesh
	  • on – On AP/Controller or RF Domain
	  • <DEVICE-OR-DOMAIN-NAME – On AP/Controller/RF Domain name

radio {detail|on|statistics|tspec}	Radio related commands. All parameters are optional. • on – On AP/Controller or RF Domain • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/RF Domain name • detail <AA-BB-CC-DD-EE-FF> <1-3>|<WORD> – Displays detailed information about a radio MAC • tspec <AA-BB-CC-DD-EE-FF> <1-3>|<WORD> – Displays detailed TSPEC information on a radio • <AA-BB-CC-DD-EE-FF> <1-3>|<WORD> – Specifies the MAC address of an AP • <1-3> – Specifies the radio interface index between 1 and 3 • <WORD> – Radio ID in the form AA-BB-CC-DD-EE-FF:RX • statistics {detail| on <DEVICE-OR-DOMAIN-NAME> |rf {on <DEVICE-OR-DOMAIN-NAME>}|traffic {on <DEVICE-OR-DOMAIN-NAME>|window-data}} – Displays statistics for all radios • rf – Displays information about RF related statistics • traffic – Displays data traffic related statistics The following parameters are common for the above: • on – On AP/Controller or RF Domain • <DEVICE-OR-DOMAIN-NAME – On AP/Controller/ RF Domain name • on – On AP/Controller or RF Domain • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/RF Domain name • detail <AA-BB-CC-DD-EE-FF> <1-3>|<WORD> – Displays detailed statistical information about a radio • window-data – Displays Window stats (historical data over a time window) • <AA-BB-CC-DD-EE-FF <1-3> – Specifies a client MAC address • <1-3> – Specifies a radio interface index between 1 and 3 • <WORD> – Specifies the radio window-stats id in the form of a MAC followed by the interface number and window number: For ex;. AA-BB-CC-DD-EE-FF:R1:W1
regulatory [channel-info <WORD>|country-code <WORD>| device-type]	• channel-info <WORD> – Displays channel information • country-code – Displays the 2 letter ISO-3166 country code • device-type [ap650|ap7131|rfs4000] <WORD> – Displays device information based on the device type • ap650 <WORD> – Displays AP650 information • ap7131 <WORD> – Displays AP7131 information • rfs4000 <WORD> – Displays the RFS4011 wireless controller model that houses radios
sensor- server {on <DEVICE-OR-DOMAIN-NAME>}	Displays information about AirDefense sensor server configuration • on – On AP/controller or RF Domain • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/ RF Domain name

unsanctioned aps {detail|statistics} {on <DEVICE-OR-DOMAIN-NAME>}	Displays information about unauthorized APs Detected
	• aps – Lists detected unauthorized APs
	  • detailed – Detailed information
	  • statistics – Displays channel statistics
	The following parameters are common for the above:
	  • on – On AP/controller or RF Domain
	  • <DEVICE-OR-DOMAIN-NAME – On AP/Controller/ RF Domain name
	• on – On AP/Controller or RF Domain
	  • <DEVICE-OR-DOMAIN-NAME – On AP/Controller/ RF Domain name

wips [event-history {on <DEVICE-OR-DOMAIN-NAME> |client-blacklist	Displays WIPS parameters
	• event-history {on <DEVICE-OR-DOMAIN-NAME>} – Displays an event history
	• client-blacklist – Displays details about blacklisted clients
	  • on – On AP/Controller or RF Domain
	  • <DEVICE-OR-DOMAIN-NAME – On AP/Controller/ RF Domain name

wlan {config|detail <WLAN>|on| policy-mapping|statistics|usage-mappings}	Displays wireless LAN parameters. The following information is displayed:
	• config – Displays the WLAN configuration
	• detail – Displays detailed configuration of specified WLAN configuration
	  • WLAN – WLAN name
	• policy-mappings – Displays the policy mappings for various WLANs
	• usage-mappings – Lists of all devices and profiles using the WLAN
	• statistics {WLAN|detail|on|traffic} – Displays the WLAN statistics for:
	  • WLAN – Displays WLAN for which the detailed statistics required
	  • detail – Displays detailed statistics for all WLANs
	  • on – On AP/Controller/RF Domain
	  • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/ RF Domain
	  • traffic – Displays data traffic related statistics
	• The following parameters are common for the above:
	  • on – On AP/Controller/RF Domain
	  • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/RF Domain

Example

```
rfs7000-37FABE(config)#show wireless sensor server status on ap7131-889EC4
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless unauthorized aps detailed
Number of APs seen: 1
rfs7000-37FABE(config)#
rfs7000-37FABE(config)#show wireless wips mu-blacklist
No mobile units blacklisted
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless wlan config
+-----------+---------+-----------+-------------+-----------------+-------
|    NAME   |  ENABLE |    SSID   |  ENCRYPTION |  AUTHENTICATION |    VLAN    |
```

```
+-----------+---------+-----------+-------------+-----------------+-------
| test      | Y       | test      | none        | none            | 1          |
| motorola  | Y       | motorola  | none        | none            | 1          |
| wlan1     | Y       | wlan1     | none        | none            | 1          |

rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless wlan statistics
+--------------------+----------+----------+--------+--------+--------+--
|        WLAN        | TX BYTES | RX BYTES |TX PKTS |RX PKTS |TX KBPS |RX KBPS |DROPPED
|  ERRORS |
+--------------------+----------+----------+--------+--------+--------+-
|          motorola |       0 |       0 |     0 |     0 |     0 |     0 |     0 |     0  |
|             wlan1 |       0 |       0 |     0 |     0 |     0 |     0 |     0 |     0  |
+--------------------+----------+----------+--------+--------+--------+--
Total number of wlan displayed: 2
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory channel-info 1
Center frequency for channel 1 is 2412MHz
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory country-code
ISO CODE                        NAME
-------------------------------------------------------------
  al                            Algeria
  ai                            Anguilla
  ar                            Argentina
  au                            Australia
  at                            Austria
  bs                            Bahamas
  bh                            Bahrain
  bb                            Barbados
  by                            Belarus
  be                            Belgium
  bm                            Bermuda
  bo                            Bolivia
  bw                            Botswana
  ba                            Bosnia-Herzegovina
  br                            Brazil
  bg                            Bulgaria
  ca                            Canada
  ky                            Cayman Islands
.............................................
rfs7000-37FABE(config)#

rfs7000-37FABE(config)#show wireless regulatory device-type ap650 in
-----------------------------------------------------------------------------
#  Channel Set Power(mW) Power (dBm)    Placement          DFS         CAC(mins)
-----------------------------------------------------------------------------
   1   1-13        4000      36          Indoor/Outdoor   NA             NA
  2   36-64       200       23          Indoor           Not Required   0
  3   149-165     1000      30          Outdoor          Not Required   0
  4   149-165     200       23          Indoor           Not Required   0
-----------------------------------------------------------------------------
rfs7000-37FABE(config)#
rfs4000-880DA7(config)#show wireless ap detail rfs4000-880DA7 on rfs4000-880DA7

AP: 00-23-68-88-0D-A7
 AP Name              : rfs4000-880DA7
 Location             : default
 RF-Domain            : default
 Type                 : rfs4000
 Model                : RFS-4011-11110-US
 Num of radios        : 2
 Num of clients       : 0
 Last Smart-RF time   : not done
 Stats update mode    : auto
 Stats interval       : 6
 Radio Modes          :
```

```
     radio-1          : wlan
     radio-2          : wlan
 Country-code         : not-set
 Site-Survivable      : True
 Last error           :
 Fault Detected       : False

rfs4000-880DA7(config)#

rfs4000-880DA7(config)#show wireless ap load-balancing on default/rfs4000-880DA7

AP: 00-23-68-88-0D-A7
Client requests on 5ghz   : allowed
Client requests on 2.4ghz : allowed

Average AP load in neighborhood               : 0 %
Load on this AP                               : 0 %
Total 2.4ghz band load in neighborhood        : 0 %
Total 5ghz band load in neighborhood          : 0 %
Configured band ratio 2.4ghz to 5ghz          : 1:1
Current band ratio 2.4ghz to 5ghz             : 0:0
Average 2.4ghz channel load in neighborhood   : 0 %
Average 5ghz channel load in neighborhood     : 0 %
Load on this AP's 2.4ghz channel              : 0 %
Load on this AP's 5ghz channel                : 0 %

Total number of APs displayed: 1
rfs4000-880DA7(config)#

rfs4000-880DA7(config)#show wireless ap on default
------------------------------------------------------------------------------
MODE        : radio modes - W = WLAN, S=Sensor, ' ' (Space) = radio not present
------------------------------------------------------------------------------
AP-NAME    AP-LOCATION      RF-DOMAIN     AP-MAC   #RADIOS  MODE #CLIENT      LAST-
CAL-TIME
------------------------------------------------------------------------------
rfs4000-880DA7   default    default 00-23-68-88-0D-A7   2   W-W    0             not
done
------------------------------------------------------------------------------
Total number of APs displayed: 1
rfs4000-880DA7(config)#
```

6.1.49 wwan

show commands

Displays wireless WAN status

Supported in the following platforms:

- RFS4000
- RFS6000

Syntax

```
show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}	• configuration – Displays wireless WAN configuration information
	• status – Displays wireless WAN status information
	  • on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF Domain
	  • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/RF Domain name

Example

```
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)*#show wwan configuration on rfs4000-
880DA7
>>> WWAN Configuration:
+-----------------------------------------
|  Access Port Name : isp.cingular
|  User Name        : testuser
|  Cryptomap        : map1
+-----------------------------------------
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#

rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#show wwan status on rfs4000-880DA7
>>> WWAN Status:
+-----------------------------------------
|  State : ACTIVE
|  DNS1  : 209.183.54.151
|  DNS2  : 209.183.54.151
+-----------------------------------------
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#
```

CHAPTER 7 PROFILES

Profiles enable administrators to assign a common set of configuration parameters and policies to controllers and Access Points. Profiles can be used to assign common or unique network, wireless and security parameters to Wireless Controllers and Access Points across a large, multi segment site. The configuration parameters within a profile are based on the hardware model the profile was created to support. The controller supports both default and user defined profiles implementing new features or updating existing parameters to groups of Wireless Controllers or Access Points. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

The system maintains a couple of default profiles. The default profile is applied to the wireless controller automatically, and default AP profiles are applied to the APs that are automatically discovered by the wireless controller. After adoption, if a change is made in one of the parameters in the profile, that change is reflected across all the APs using the same profile.

User defined profiles are manually created for each supported Wireless Controller and Access Point model. User defined profiles can be manually assigned or automatically assigned to Access Points.

- AP650 – Adds an AP650 access point profile
- AP7131 – Adds an AP7131 access point profile
- RFS4000 – Adds an RFS4000 wireless controller profile
- RFS6000 – Adds an RFS6000 wireless controller profile
- RFS7000 – Adds an RFS7000 wireless controller profile

Each default and user defined profile contains policies and configuration parameters. Changes made to these parameters are automatically inherited by the devices assigned to the profile.

```
rfs7000-37FABE(config)#profile rfs7000 default-rfs7000
rfs7000-37FABE(config-profile-default-rfs7000)#


rfs7000-37FABE(config)#profile ap7131 default-ap7131
rfs7000-37FABE(config-profile-default-ap7131)#
```

7.1 Creating Profiles

NOTE: The commands present under 'Profiles' are also available under the 'Device mode'. The additional commands specific to the 'Device mode' are listed separately. Refer *Chapter 7, Device Mode Commands* for more information.

Table 7.1 Summarizes Profile Commands

Table 7.1 *Profile Commands*

Command	Description	Reference
aaa	Configures AAA settings	*page 7-4*
ap-upgrade	Enables an automatic adopted AP firmware upgrade	*page 7-10*
arp	Configures the static address resolution protocol	*page 7-6*
auto-learn-staging-config	Enables network configuration learning of the devices	*page 7-8*
autoinstall	Configures auto install feature	*page 7-9*
bridge	Configures bridge specific commands	*page 7-12*
cdp	Performs the *Cisco Discovery Protocol* (CDP) on a device	*page 7-21*
cluster	Defines the cluster-name	*page 7-22*
configuration-persistence	Enables persistence of configuration across reloads	*page 7-24*
controller	Configures a WLAN controller	*page 7-25*
crypto	Configures crypto settings	*page 7-27*
dscp-mapping	Configures an IP DSCP to 802.1p priority mapping for untagged frames	*page 7-41*
email-notification	Configures email notification	*page 7-42*
enforce-version	Checks the firmware versions of devices before inter-operating	*page 7-44*
events	Displays system event messages	*page 7-46*
interface	Selects an interface to configure	*page 7-54*
ip	Configures a selected Internet Protocol component	*page 7-47*
led	Turns device LEDs on/off	*page 7-83*
legacy-auto-downgrade	Enables a legacy device firmware auto downgrade	*page 7-84*
legacy-auto-update	Enables a legacy device firmware auto update	*page 7-85*
lldp	Configures *Link Layer Discovery Protocol* (lldp)	*page 7-86*
load-balancing	Configures load balancing parameters	*page 7-87*
local	Creates a local user authentication database for VPN	*page 7-89*

Table 7.1 *Profile Commands*

Command	Description	Reference
logging	Modifies message logging facilities	*page 7-90*
mac-address-table	Configures the MAC address table	*page 7-92*
mint	Configures the MiNT protocol	*page 7-93*
misconfiguration-recovery-time	Verifies controller connectivity after the configuration is received	*page 7-96*
monitor	Enables critical resource monitoring	*page 7-97*
neighbor-inactivity-timeout	Configures neighbor inactivity timeout factor	*page 7-98*
neighbor-info-interval	Configures neighbor information exchange interval	*page 7-99*
no	Negates a command or sets its default values	*page 7-100*
noc	Configurse the noc related settings	*page 7-101*
ntp	Configures a NTP server	*page 7-102*
power-config	Configures the power mode feature	*page 7-104*
preferred-controller-group	Specifies the controller group the system prefers for adoption	*page 7-103*
radius	Configures device level radius authentication parameters	*page 7-105*
rf-domain-manager	Enables the rf-domain-manager feature	*page 7-106*
service	Sets service commands	*page 7-107*
spanning-tree	Configures spanning tree commands	*page 7-108*
use	Defines the settings used by this feature	*page 7-111*
vpn	Configures VPN settings	*page 7-113*
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication	*page 7-114*

7.1.1 aaa

Creating Profiles

Configures VPN AAA authentication settings on the device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
aaa vpn-authentication
aaa vpn-authentication [primary|secondary] <A.B.C.D> key [0 <WORD>|2
<WORD>|<WORD>] {auth-port <1024-65535>}
```

Parameters

vpn-authentication [primary|secondary] <A.B.C.D> key [0 <WORD>|2 <WORD>|<WORD>] {auth-port <1024-65535>}	Configures RADIUS settings • primary – Sets primary RADIUS server settings • secondary – Sets secondary RADIUS server settings The following parameters are common for the above: • <A.B.C.D> – Specifies the IP address for the RADIUS server • key [0|2|<WORD>] – Sets the RADIUS client preshared key; this key should match the RADIUS server • 0 – Enter a clear text secret • 2 – Enter an encrypted secret • <WORD> – Specifies the shared secret up to 32 characters • {auth-port <1024-65535>} – Sets the RADIUS server authentication port. Enter a port value between 1024 and 65535.

Usage Guidelines

Use an AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#aaa vpn-authentication secondary
172.16.10.8 key symbo123l authport 1025
rfs7000-37FABE(config-profile-default-rfs7000)#show contex
profile rfs7000 default-rfs7000
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 aaa vpn-authentication secondary 1.2.3.4 key 0 motorolasolutions123 authport 1025
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
```

```
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 use firewall-policy default
 service pm sys-restart
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.2 arp

Creating Profiles

Configures the address resolution protocol parameters.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
arp [<IP>|timeout
arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|vlan <VLAN>] {[dhcp-server|router]}
arp timeout <TIME>
```

Parameters

<IP> <MAC> `arpa [<L3-INTERFACE-NAME>|vlan <VLAN>] {[dhcp-server|router]}`	Configures a static ARP entry for a given IPv4 IP address.
	• <IP> – The static IP adderss to configure the ARP entry for
	• <MAC> – The MAC address to be associated with the IP and SVI
	• arpa – The type of ARP.
	  • <L3-INTERFACE-NAME> – Sets the router interface name
	  • vlan <VLAN> – Sets a switch vlan interface where <VLAN> is the SVI interface name.
	  • dhcp-server – Optional. Sets the ARP entry for a dhcp-server
	  • router – Optional. Sets the ARP entry for a router.

timeout <TIME>	Sets the ARP timeout value. • <TIME> – Sets the ARP entry timeout value in seconds. Enter a value in the range 15-86400 seconds.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#arp timeout 2000
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 arp timeout 2000
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
rfs7000-37FABE(config-profile-default-rfs7000)#arp 172.16.10.10 45-bc-22-38-16-3F
arpa vlan 3 dhcp-server
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 arp 172.16.10.10 45-bc-22-38-16-3F arpa vlan3 dhcp-server
 arp timeout 2000
 no autoinstall configuration
```

```
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
interface me1
interface ge1
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
```

7.1.3 auto-learn-staging-config

Creating Profiles

Enables network configuration learning of the devices which come for adoption automatically

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
auto-learn-staging-config
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#auto-learn-staging-config
```

7.1.4 autoinstall

Creating Profiles

Autoinstalls the controller image

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
autoinstall [configuration|firmware]
```

Parameters

configuration	Installs configuration setup parameters automatically
firmware	Installs firmware image automatically

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#autoinstall configuration
rfs7000-37FABE(config-profile-default-rfs7000)#autoinstall firmware version 5.1.0.0-
072R
```

7.1.5 ap-upgrade

Creating Profiles

Enables an automatic firmware upgrade for an adopted AP

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap-upgrade [auto|count <1-20>]
```

Parameters

auto	Enables automatic adopted AP firmware upgrade
count <1-20>	Sets the concurrent upgrade limit • <1-20> – Enter the number of concurrent upgrades that can be performed.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#ap-upgrade count 7
```

7.1.6 bridge commands

Creating Profiles

Configures the Ethernet Bridging commands.

Table 7.2 *Bridging Commands*

Command	Description	Reference
bridge	Configures the Ethernet Bridging parameters	page 7-12

7.1.6.1 bridge

bridge commands

Configures bridge specific commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Switch Note: The interfaces mentioned below are supported as follows:

- ge <index> – RFS7000 and RFS4000 supports 4 GEs, RFS6000 supports 8 GEs
- me1– Only supported on RFS7000 and RFS6000

Syntax

```
bridge vlan <1-4095>
```

Parameters

vlan <1-4095>	Enter a VLAN index value between 1 and 4095

Usage Guidelines

Creating customized filter schemes for bridged networks limits the amount of unnecessary traffic processed and distributed by the bridging equipment.

If a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#bridge vlan 5
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.6.2 bridge-vlan-mode commands

bridge commands

Table 7.3 Summarizes bridge-vlan-mode commands

Table 7.3 *bridge-vlan commands*

Command	Description	Reference
bridging-mode	Configures how packets on this VLAN are bridged.	*page 7-14*
description	Defines the VLAN description	*page 7-15*
edge-vlan	Enables edge VLAN mode	*page 7-16*
ip	Configures the selected Internet Protocol (IP) component	*page 7-16*
no	Negates a command or sets its default values	*page 7-18*
stateful-packet-inspection-12	Enables a stateful packet inspection in the layer2 firewall	*page 7-18*
use	Uses preconfigured access lists with this bridge policy.	*page 7-20*

7.1.6.2.1 bridging-mode

bridge-vlan-mode commands

Cofigures how the packets on the selected VLAN are bridged.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

Parameters

auto|isolated-tunnel|local|tunnel	• auto – Choose bridging mode automatically to match WLAN, vlan, and bridging-mode configuration • isolated-tunnel – Bridge packets between local ethernet ports and any local radios, and pass tunneled packets through without detunneling them • local – Bridge packets normally, between the local ethernet ports and local radios (if any) • tunnel – Bridge packets between local ethernet ports, any local radios, and tunnels to other APs and wireless-switches

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#bridging-mode isolated-
tunnel
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

7.1.6.2.2 description

bridge-vlan-mode commands

Sets a description of a Bridged VLAN.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
description <WORD>
```

Parameters

description <WORD>	Defines the VLAN description

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#description "This is a
description for the bridged VLAN"
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#show context
 bridge vlan 1
  description This\ is\ a\ description\ for\ the\ bridged\ VLAN
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
```

7.1.6.2.3 edge-vlan

bridge-vlan-mode commands

Enables the edge VLAN mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
edge-vlan
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#edge-vlan
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

7.1.6.2.4 ip

bridge-vlan-mode commands

Configures the selected Internet Protocol (IP) component

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip [arp trust|dhcp trust|igmp]
ip igmp snooping {mrouter|querier|unknown-multicast}
ip igmp snooping mrouter [interface <WORD>|learn pim-dvrp]
ip igmp snooping querier {address <A.B.C.D>|max-response-time <1-25>|timer expiry <60-
300>|version <1-3>}
```

Parameters

arp trust	Configures an ARP component • trust – Trust ARP responses on VLAN
dhcp trust	Configures DHCP components • trust – Trust DHCP responses on a VLAN
igmp snooping {mrouter(interface <WORD>|learn|querier {address <A.B.C.D>| max-response-time <1-25>|timer expiry <60-300>|version <1-3>}|unknown-multicast}	Configures Internet Group Management Protocol (IGMP) • snooping {mrouter|querier|unknown-multicast} – Configures IGMP snooping • mrouter [interface <WORD>|learn pim-dvrp] – Configures a multicast router • interface <WORD> – Specifies the interfaces to be configured • learn pim-dvrp – Sets the multicast router learning protocol • pim-dvrp – Learns mrouter through PIM or DVRP protocols. • querier {address <A.B.C.D>|max-response-time <1-25>|timer expiry<60-300>|version <1-3>} – Configures IGMP querier • address <A.B.C.D> – Configures an IGMP querier source IP address • <A.B>C.D> – Specifies an IGMP querier source IP address • max-response-time <1-25> – Configures an IGMP querier maximum response time (sec) • <1-25> – Specifies an IGMP querier maximum response time (sec) • timer expiry <60-300> – Configures the IGMP querier timer • expiry <60-3000> – Specifies an IGMP querier other querier time out (sec) • version <1-3> – Configures an IGMP version • <1-3> – Specifies the IGMP the version • unknown-multicast – Forwards unknown multicast packets

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#ip arp trust
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#ip dhcp trust
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#

rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#ip igmp snooping mrouter
learn pim-dvmrp
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#ip igmp snooping mrouter
interface ge1
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#ip igmp snooping querier
max-response-time 5
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#ip igmp snooping querier
version 2
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#ip igmp snooping querier
timer expiry 89
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#
```

7.1.6.2.5 no

bridge-vlan-mode commands

Negates a command or set its defaults

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [description|edge-vlan|extended-vlan|ip|overlaid-vlan| stateful-packet-
inspection-l2|use]
```

Parameters

description	Removes VLAN description
edge-vlan	Enables edge VLAN mode
extended-vlan	Enables extended VLAN mode
ip	Configures the selected Internet Protocol (IP) component
overlaid-vlan	Disables overlaid VLAN mode
stateful-packet-inspection-l2	Disables stateful packet inspection in layer2 firewall
use	Uses preconfigured access lists with this bridge policy

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#no description
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-5)#

rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#no ip igmp snooping
mrouter interface ge1
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#

rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#no ip igmp snooping
mrouter learn pim-dvmrp
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#

rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#no ip igmp snooping
querier max-response-time
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#

rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#no ip igmp
querier version
rfs7000-37FABE(config-profile defaultrfs7000-bridge-vlan-5)#
```

7.1.6.2.6 stateful-packet-inspection-12

bridge-vlan-mode commands

Enables a stateful packet inspection at a layer2 firewall

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
stateful-packet-inspection-l2
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile defalut-rfs7000-bridge-vlan-2)#stateful-packet-
inspection-l2
rfs7000-37FABE(config-profile defalut-rfs7000-bridge-vlan-2)#
```

7.1.6.2.7 use

bridge-vlan-mode commands

Uses preconfigured access lists with this bridge policy.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
use [ip-access-list|mac-access-list]
use ip-access-list ext-vlan out <IP-ACCESS-LIST>
use mac-access-list ext-vlan out <MAC-ACCESS-LIST>
```

Parameters

ip-access-list|mac-access-list]	• ip-access-list – Uses IP access list
	• mac-access-list – Uses MAC access list
	  • ext-vlan – Enables extended-VLAN on the selected access list
	  • out – Applies ACL on the outgoing packets
	  • <IP-ACCESS_LIST> <MAC-ACCESS-LIST> – Specify the access list name as IP ACL or MAC ACL

Example

```
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#use ip-access-list ext-
vlan out test
rfs7000-37FABE(config-profile default-rfs7000-bridge-vlan-1)#
```

NOTE: The commands write, clrscr, help, exit, end,commit, do revert, service, and show are common for all the commands. For more information, see *Chapter 5, COMMON COMMANDS*.

7.1.7 cdp

Creating Profiles

Operates the *Cisco Discovery Protocol* (CDP) on the device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
cdp [holdtime <10-1800>|run|timer <5-900>]
```

Parameters

holdtime <10-1800>	Specifies the holdtime value transmitted in CDP packets between 10 and 1800 seconds
run	Enables CDP sniffing and transmit globally
timer <5-900>	Specifies the timer value between 5 and 900 seconds

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#cdp run
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default)#cdp holdtime 11
rfs7000-37FABE(config-profile-default)#

rfs7000-37FABE(config-profile-default)#cdp timer 15
rfs7000-37FABE(config-profile-default)#
```

7.1.8 cluster

Creating Profiles

Sets the cluster configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
cluster [auto-revert|auto-revert-delay|handle-stp|member|mode|name]
cluser member [ip <A.B.C.D>|vlan <1-4094>]
cluster mode [active|standby]
cluster name <WORD>
```

Parameters

auto-revert	Enables auto-revert
auto-revert-delay <1-1800>	Configures auto-revert-delay between 1 and 1800 minutes
handle-stp	Configures STP convergence

member [ip <A.B.C.D>|vlan <1-4094>]	Adds a cluster member
	• ip <A.B.C.D> – Sets the IP address of the cluster member
	  • <A.B.C.D> – Specifies the IP address to configure
	• vlan <1-4094> – Sets the VLAN on which cluster members are reachable
	  • <1-4094> – Specifies the VLAN index between 1- 4094

mode [active|standby]	Configures the cluster mode as either active or standby • active – Active mode • standby – Standby mode
name <WORD>	Configures cluster name

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#cluster name cluster1
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#cluster member ip 172.16.10.3
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#cluster mode active
rfs7000-37FABE(config-profile-default-rfs7000)#
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  description Vlan1
.........................................
```

```
 cluster name cluster1
 cluster member ip 172.16.10.3
 cluster member vlan 1

rfs7000-37FABE(config-profile-default-rfs7000)#cluster auto-revert-delay 10
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.9 configuration-persistence

Creating Profiles

Enables persistence of configuration across reloads

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- RFS71xx
- AP650
- AP6511
- AP6532

Syntax

```
configuration-persistence {secure}
```

Parameters

secure	Optional. Ensures that parts of the file that contain security related information are not written during a reload.

Example

```
rfs7000-37FABE(config-profile-default)#configuration-persistence secure
rfs7000-37FABE(config-profile-default)#
```

7.1.10 controller

Creating Profiles

Configures a WLAN controller information. Sets the controller to be a part of a group of controllers, sets if the controller is a part of a pool of controllers, etc.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- RFS71xx
- AP650
- Ap6511
- AP6532

Syntax

```
controller [group <CONTROLLER-GROUP>]
controller vlan <1-4094>
controller host [<IP>|<HOSTNAME>] {[level [1|2]|pool <1-2>]}
```

Parameters

[group|host|vlan]	• group – Enter the address of the controller group to which this controller will belong
	• host – The address of the controller that is to be configured
	  • <IP> – Enter the IP adddress of the controller
	  • <HOSTNAME> – Enter the hostname of the controller
	The following parameters are common to <IP> and <HOSTNAME>:
	  • level [1|2] – Enter the routing level. There are two routing levels you can select from. Level1 is for local routing and Level 2 is for inter-site routing
	  • pool <1-2> – Enter the controller pool to which this controller belongs to. Default value is 1.
	• vlan <1-4094> – Enter the VLAN on which the controller can be reached. Enter a VLAN ID in the range 1 and 4094.

Example

```
rfs7000-37FABE(config-profile-defaullt)#controller group test
rfs7000-37FABE(config-profile-default-rfs7000)#controller host 1.2.3.4 pool 2
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
```

```
interface ge4
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
use firewall-policy default
controller host 1.2.3.4 pool 2
controller group test
service pm sys-restart
```

7.1.11 crypto

Creating Profiles

Use crypto to define system level local ID for ISAKMP negotiation and to enter the ISAKMP Policy, ISAKMP Client or ISAKMP Peer command set.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map set associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map set associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable SA exists, it is used for transmission. Otherwise, IKE is used to establish an SA with the peer. If no SA exists (and the crypto map entry is "respond only"), the packet is discarded.

When a secured packet arrives on an interface, its SPI is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
crypto [ipsec|isakmp|map|pki]

crypto ipsec [security-association|transform-set]
crypto ipsec security-association lifetime [kilobyte|seconds] <lifetime>
crypto ipsec transform-set <transform-set-tag> [ah-md5-hmac|
ah-sha-hmac|esp-3des|esp-aes|esp-aes-192|esp-aes-256|esp-des|
esp-md5-hmac|esp-sha-hmac]

crypto isakmp [aggresive-mode-peer|client|keepalive|key|policy]
crypto isakmp client configuration group default
crypto isakmp keepalive <10-3600>
crypto isakmp key [0 <WORD>|2 <WORD>|<WORD>] address <A.B.C.D>
[address <IP>|hostname <HOST>]
crypto isakmp aggresive-mode-peer [address <IP>|dn <distinguished-name>|hostname
<HOST>] key [0 <WORD>|2 <WORD>|<WORD>]
crypto isakmp policy <ISAKMP-POLICY>

crypto map <crypto-map-tag> <1-1000> [ipsec-isakmp|ipsec-manual] {dynamic}

crypto pki import crl <WORD> URL <1-168>
```

Parameters

ipsec	Configures IPSEC policies

[security-association| transform-set]	Configures IPSEC security associations and transform set.
	• security-association – Defines the lifetime (in kilobytes and/or seconds) of the IPSec SAs created
	  • lifetime [kilobyte | seconds] – Specifies how many kilobyte/ seconds an IKE SA lasts before it expires. Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association
	  • kilobytes – Volume-based key duration, the minimum is 500 KB and the maximum is 2147483646 KB
	  • seconds – Time-based key duration, the minimum is 90 seconds and the maximum is 2147483646 seconds
	• transform-set [set name] – Uses the crypto ipsec transform-set command to define the transform configuration (authentication and encryption) for securing data
	  • ah-md5-hmac – AH-HMAC-MD5 transform
	  • ah-sha-hmac – AH-HMAC-SHA transform
	  • esp-3des – ESP transform using 3DES cipher (168 bits)
	  • esp-aes – ESP transform using AES cipher
	  • esp-aes-192 – ESP transform using AES cipher (192 bits)
	  • esp-aes-256 – ESP transform using AES cipher (256 bits)
	  • esp-des – ESP transform using DES cipher (56 bits)
	  • esp-md5-hmac – ESP transform using HMAC-MD5 auth
	  • esp-sha-hmac – ESP transform using HMAC-SHA auth
	The transform set is then assigned to a crypto map using the map's set transform-set command.

isakmp [aggresive-mode-peer|client|keepalive|key|policy]	Configures the *Internet Security Association and Key Management Protocol* (ISAKMP) policy
	• aggressive-mode-peer [address|dn|hostname] – Defines the aggressive mode attributes
	  • address – The IP address is the identity of the remote peer
	  • dn – The identity of the remote peer is the distinguished name
	  • hostname –The hostname is the identity of the remote peer
	• client configuration group default – Leads to the config-crypto group instance
	  • configuration – Defines the configuration set at the client
	  • group – -Defines the group (currently only one is supported)
	  • default – Default the group tag
	• keepalive <10-3600> – Sets a keepalive interval for use with remote peers. It defines the number of seconds between DPD messages.
	• key [0|2|<WORD>] address <A.B.C.D> – Sets a pre-shared key for a remote peer
	  • 0 <WORD> – Enter a clear text key
	  • 2 <WORD> – Enter an encrypted key
	  • <WORD> – Sets a key of size minimum 8 characters
	  • address <A.B.C.D> – Defines a shared key with an IP address
	• policy <ISAKMP-POLICY> – Sets a policy for a ISAKMP protection suite

map <crypto-map-tag> <1-1000> [ipsec-isakmp| ipsec-manual] {dynamic}	Enter a crypto map
	• name <name> – Names the crypto map entry (cannot exceed 32 characters)
	  • <1-1000> – Defines the sequence to insert into the crypto map entry
	  • ipsec-isakmp – IPSEC w/ISAKMP
	  • ipsec-manual – IPSEC w/manual keying
	  • dynamic – Dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration

pki import crl <WORD> URL <1-168>	Configures certificate parameters. The public key infrastructure is a protocol that creates encrypted public keys using digital certificates from certificate authorities.
	• import – Imports a trustpoint related configuration
	  • crl – Certificate revocation list
	  • <WORD> – Imports a trustpoint including either a private key and server certificate or a CA certificate or both
	  • URL <1-168> – URL to get certificate from URLS:
	  tftp://<IP>/path/file
	  ftp://<user>:<passwd>@<IP>/path/file
	  • -<1-168> – Sets the duration to replay the command (between 1 and 168 hours)

Usage Guidelines

If no peer IP address is configured, the manual crypto map is not valid and not complete. A peer IP address is required for manual crypto maps. To change the peer IP address, the no set peer command must be issued first, then the new peer IP address can be configured.

A peer address can be deleted with a wrong ISAKMP value. Crypto currently matches only the IP address when a no command is issued.

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto isakmp key 12345678
address 4.4.4.4
```

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto ipsec transform-set tpsec-tag1
ah-md5-hmac
rfs7000-37FABE(config-profile-default-rfs7000-transform-set-tpsec-tag1)#

rfs7000-37FABE(config-profile-default-rfs7000)#crypto map map1 10 ipsec-manual
dynamic
% Error: Remote Configuration not allowed for Manual Crypto Map
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#crypto map map1 10 ipsec-isakmp
dynamic
rfs7000-37FABE(config-profile-default-rfs7000-cryptomap-map1 10)#

rfs7000-37FABE(config-profile-default-rfs7000)#crypto isakmp client configuration
group default
rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#
rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#?
Crypto Client Config commands:
  dns       Domain Name Server
  wins      Windows name server

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#
```

7.1.12 isakmp-policy

Use the (config) instance to configure ISAKMP policy related configuration commands. To navigate to the config-isakmp-policy instance, use the following commands:

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto isakmp policy test
rfs7000-37FABE(config-profile-default-rfs7000-isakmp-policy-test)#?
Crypto Isakmp Config commands:
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-isakmp-policy-test)#
```

Table 7.4 Summarizes isakmp-policy commands

Table 7.4 *isakmp-policy Commands*

Command	Description	Reference
authentication	Authenticates rsa-sig and pre-share keys	*page 7-32*
encryption	Configures the encryption level of the data transmitted using the `crypto-isakmp` command	*page 7-33*
group	Specifies the Diffie-Hellman group (1 or 2) used by the IKE policy	*page 7-34*
hash	Specifies the hash algorithm	*page 7-35*
lifetime	Specifies how long an IKE SA is valid before it expires	*page 7-36*
no	Negates a commnd or sets its default value	*page 7-37*

7.1.12.1 authentication

isakmp-policy

~~Authenticates and pre share keys~~Sets the authentication method for the cryptography suite

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
authentication [pre-share|rsa-sig]
```

Parameters

pre-share	Use the pre-shared key
rsa-sig	Use the Rivest-Shamir-Adleman (RSA) Signature

Example

```
rfs7000-37FABE(config-isakmp-policy-test)#authentication rsa-sig
rfs7000-37FABE(config-prfile-default-rfs7000-isakmp-policy-test)#show context
 crypto isakmp policy test
  authentication rsa-sig
```

7.1.12.2 encryption

isakmp-policy

Configures the encryption level transmitted using the `crypto-isakmp` command

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
encryption [3des|aes|aes-192|aes-256|des]
```

Parameters

[3des|aes|aes-192| aes-256|des]	Sets an encryption algorithm for the protection suite • 3des – Triple data encryption standard • aes – Advanced encryption standard (128 bit keys) • aes-192 – Advanced encryption standard (192 bit keys) • aes-256 – Advanced encryption standard (256 bit keys) • des – Data encryption standard (56 bit keys)

Example

```
rfs7000-37FABE(config-isakmp-policy-test)#encryption 3des
rfs7000-37FABE(config-isakmp-policy-test)#
```

7.1.12.3 group

isakmp-policy

Specifies the Diffie-Hellman group (1 or 2) used by the IKE policy to generate keys (which is then used to create an IPSec SA)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
group [1|2|5]
```

Parameters

[1|2|5]	• 1– Diffie-Hellman group 1 • 2 – Diffie-Hellman group 2 • 5 – Diffie-Hellman group 5

Usage Guidelines

The local IKE policy and the peer IKE policy must have matching group settings for negotiation to be successful.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-isakmp-policy-test)#group 1
rfs7000-37FABE(config-profile-default-rfs7000-isakmp-policy-test)#show context
 crypto isakmp policy test
  authentication rsa-sig
  group 1
```

7.1.12.4 hash

isakmp-policy

Specifies the hash algorithm used to authenticate data transmitted over the IKE SA

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
hash [md5|sha]
```

Parameters

md5	Uses the MD5 hash algorithm
sha	Uses the SHA hash algorithm

Example

```
rfs7000-37FABE(config-isakmp-policy-test)#hash sha
```

7.1.12.5 lifetime

isakmp-policy

Specifies how long an IKE SA is valid before it expires

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
lifetime <WORD>
```

Parameters

lifetime <WORD>	Specifies how many seconds an IKE SA lasts before it expires. A time stamp (in seconds) can be configured between 60 and 2147483646.

Example

```
rfs7000-37FABE(config-isakmp-policy-test)#lifetime 2000
rfs7000-37FABE(config-profile-default-rfs7000-isakmp-policy-test)#show context
 crypto isakmp policy test
  authentication rsa-sig
  group 1
  lifetime 2000
rfs7000-37FABE(config-isakmp-policy-test)#
```

7.1.12.6 no

isakmp-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [authentication|encryption|group|hash|lifetime]
```

Parameters

[authentication|encryption|group|hash|lifetime]	• authentication – Sets a default authentication method • encryption – Sets an encryption algorithm for protection suite • group – Sets the default DH group to 2 • hash – Sets the hash algorithm for protection suite • lifetime – Sets the lifetime for ISAKMP security association

Example

```
rfs7000-37FABE(config-isakmp-policy-test)#no authentication
rfs7000-37FABE(config-isakmp-policy-test)#no lifetime
```

NOTE: The commands clrscr, commit, exit, help, write, revert, service and show are common commands. Refer to *Chapter 5, COMMON COMMANDS* for more information.

7.1.13 crypto-group

Creating Profiles

Use the (config) instance to configure crypto-group related configuration commands:

```
rfs7000-37FABE(config-profile-default-rfs7000)#crypto isakmp client configuration
group default
rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#
rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#?
Crypto Client Config commands:
  dns       Domain Name Server
  wins      Windows name server

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)
```

Table 7.5 Summarizes crypto-group commands

Table 7.5 *crypto-group Commands*

Command	Description	Reference
dns	Configures domain name server settings	*page 7-39*
wns	Configures windows name server settings	*page 7-40*

7.1.13.1 dns

crypto-group

Configures domain name server settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dns <IP>
```

Parameters

<IP>	Sets the IP address for the domain name server

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#dns 171.16.10.6
rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#show context
 crypto isakmp client configuration group default
  wins 1.2.3.4
  dns 171.16.10.6
```

7.1.13.2 wns

crypto-group

Configures the Windows name server settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wns <A.B.C.D>
```

Parameters

<A.B.C.D>	Sets the IP address for Windows name server

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#wns 172.16.10.8
rfs7000-37FABE(config-profile-default-rfs7000-crypto-group)#show context
 crypto isakmp client configuration group default
  wins 1.2.3.4
  dns 171.16.10.6
```

7.1.14 dscp-mapping

Creating Profiles

Configures IP DSCP to 802.1p priority mapping for untagged frames

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dscp-mapping <WORD> priority <0-7>
```

Parameters

<WORD>	Enter a DSCP value of a received IP packet
priority <0-7>	Priority used for the packet if untagged. • <0-7> – Specifies the 802.1p priority value between 0 and 7

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#dscp-mapping 20 priority 7
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 dscp-mapping 20 priority 7
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
```

7.1.15 email-notification

Creating Profiles

Configures email notification

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
email-notification [host <IP>|recipient <EMAIL>]
email-notification host <IP> sender <EMAIL> {port <1-65535||username <WORD>}
```

Parameters

[host|recipient]]
host[sender {port|username}
	• host <IP>– Configures the host SMTP server
	  • <IP> – The IP address of the SMTP server.
	  • sender <EMAIL> – configures sender email address
	  • <EMAIL> – Enter the email address of the sender
	  • port – Optional. Enter the port number. The port number can be within 1-65535
	  • username – Optional. Enter the SMTP user name
	• recipient <EMAIL> – Configures the address of recipient email address
	  • <EMAIL> – Enter the email address of the recipient

Example

```
rfs7000-37FABE(config-profile-defaullt)#email-notification recipient
test@motorolasoultions.com
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 dscp-mapping 20 priority 7
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
```

```
 qos trust 802.1p
use firewall-policy default
email-notification recipient test@motorolasolutions.com
service pm sys-restart
```

7.1.16 enforce-version

Creating Profiles

Checks the firmware versions of devices before interoperating

Supported in the following platforms:

- RFS7000
- RFS6000
- RF4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
enforce-version [adoption|cluster] [full|major|none|strict]
```

Parameters

[adoption|cluster]	• adoption – Checks the firware versions before adopting • cluster – Checks the firmware versions before clustering The following parameters are common to adoption and cluster: • full – Allows adoption/clustering only when full versions of the formware are exactly the same • major – Allows adoption/clustering only when major and minor versions are exactly the same • none – Allows adoption/clustering between any version • strict – Allows adoption/clustering when firmware versions are exactly the same

Example

```
rfs7000-37FABE(config-profile-defaullt)#enforce-version cluster full
rfs7000-37FABE(config-profile-defaullt)#enforce-version adoption major
rfs7000-37FABE(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
 dscp-mapping 20 priority 7
 no autoinstall configuration
 no autoinstall firmware
 crypto isakmp policy default
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
```

```
 qos trust 802.1p
interface ge4
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
use firewall-policy default
email-notification recipient test@motorolasolutions.com
enforce-version adoption major
enforce-version cluster full
service pm sys-restart
```

7.1.17 events

Creating Profiles

Displays system event messages

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
events [forward on|on]
```

Parameters

[forward on|on]	• forward – Forwards system event messages to the wireless controller or cluster members • on – Enables the forwarding of system events on – Generates system events on this controller

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#events forward on
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.18 ip

Creating Profiles

Configures a selected Internet Protocol component

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip [default-gateway|dns-server-forward|route|dhcp|domain-lookup|
domain-name|local|name-server|nat|routing]
ip dhcp client [hostname|persistent-lease]
ip default-gateway <A.B.C.D>
ip route <A.B.C.D/M> <A.B.C.D>
ip domain-name <WORD>
ip local pool default low-ip-address <A.B.C.D> {high-ip-address} <A.B.C.D>
ip name-server <A.B.C.D>
ip nat [inside|outside|pool]
ip nat [inside|outside] [destination|source]
ip nat [inside|outside] [destination static <A.B.C.D>[<1-65535>[[tcp |udp] <A.B.C.D>
{1-65535>}]|<A.B.C.D> {1-65535}]
ip nat [inside|outside] [source [list <IP-ACCESS-LIST> interface vlan
 <1-4094> [address <A.B.C.D> overload|overload|pool <NAT-pool> overload]|static
<A.B.C.D> <A.B.C.D>]
ip nat pool <NAT-POOL> prefix-length <1-30>
```

Parameters

default-gateway <A.B.C.D>	Configures the IP address of the default gateway • <A.B.C.D> – IP address of the next-hop router
dns-server-forward	Enables *Domain Name Service* (DNS) Forwarding
route <A.B.C.D/M> <A.B.C.D>	Establishes static routes • <A.B.C.D/M> – IP destination prefix (e.g. 10.0.0.0/8) • <A.B.C.D> – IP gateway address
dhcp client [hostname|persistent-lease]	Configures the *Dynamic Host Control Protocol* (DHCP) client and host • client – Sets the DHCP client • hostname – Includes the hostname in the DHCP request • persistent-lease – Retains last lease across reboot if DHCP server is unreachable
domain-lookup	Enables domain lookup service
domain-name <WORD>	Configures a default domain name for DNS
local pool default low-ip-address <A.B.C.D> {highest-ip-address} <A.B.C.D>	Sets an IP address range assigned to VPN clients using mode-config or IPSec with L2TP • pool default – Specifies the address range to configure • default – Default group tag • low-ip-address <A.B.C.D> – Sets lowest range for IP address • {highest-ip-address} <A.B.C.D> – Sets the highest range for IP address
name-server <A.B.C.D>	Configures the IP address of the name-server

nat[inside|outside][destination static <A.B.C.D> [<1-65535>[[tcp |udp] <A.B.C.D> {1-65535>}]|<A.B.C.D> {1-65535}]|source [list <IP-ACCESS-LIST> interface vlan <1-4094> [<A.B.C.D> overload|overload]|static <A.B.C.D> <A.B.C.D>]	*Network Address Translation* (NAT)
	• inside – Inside address translation
	• outside – Outside address translation
	The following parameters are the same for both inside and outside NAT parameters:
	• destination static – Specifies the destination address translation to configure
	  • static <A.B.C.D> – Specifies the static NAT mapping
	  • <A.B.C.D> [<1-65535>|<A.B.C.D>] – Specifies the IP address (A.B.C.D) to configure
	  • <1-65535> [tcp|udp] – Select a value between 1 and 65535 to configure as an actual outside port
	  • tcp – Transmission control protocol
	  • udp – User datatgram protocol
	The following parameters are common for both TCP and UDP:
	  • <A.B.C.D> {<1-65535>} – Specifies the outside natted IP address (A.B.C.D) to configure
	  • <1-65535> – Select a value between 1 and 65535 to configure outside natted port
	  • A.B.C.D> <1-65535> – Specifies the outside natted IP address (A.B.C.D)
	  • <1-65535> – Select a value between 1 and 65535 to configure outside natted Port
	• source – Specifies the source address translation to configure
	  • list <IP-ACCESS-LIST> – Specifies the access list describing local addresses
	  • <IP-ACCESS-LIST> interface – Specifies the access list name
	  • interface vlan – Select an Interface to configure
	  • vlan <1-4094> – Select a VLAN interface (switched virtual interface) to configure
	  • <1-4094> [address <A.B.C.D> overload|overload|pool] – Select a VLAN ID between 1 and 4094 to configure the interface
	  • address <A.B.C.D> overload – Specifies an interface IP address used for NAT
	  • overload – Enables the use of one global address for numerous local addresses.
	  • pool <NAT-POOL> overload – Sets the NAT pool
	  • <NAT-POOL> – Specifies the NAT pool
	  • static [<A.B.C.D> |<A.B.C.D> – Specifies the static local-global mapping
	  • <A.B.C.D> – Specifies the inside actual IP address (A.B.C.D) to configure
	  • A.B.C.D> – Specifies the natted IP address (A.B.C.D) to configure
	• pool <NAT-POOL> – IP address pool for NAT

	• <NAT-POOL> – Specifies the NAT pool to use • prefix-length <1-30> – Specifies the number of netmask bits
routing	Enables IP routing

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#ip default-gateway 172.16.10.9
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#ip dns-server-forward
rfs7000-37FABE(config-profile-default-rfs7000)#
rfs7000-37FABE(config-profile-default-rfs7000)#ip route 172.16.10.10/24 172.16.10.2
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#ip local pool default low-ip-address
1.2.3.4 high-ip-address 6.7.8.9
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#ip nat inside source list test
interface vlan 1 pool pool1 overload
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#ip nat pool pool1 prefix-length 9
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#?
Nat Policy Mode commands:
  address  Specify addresses for the nat pool
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)
```

7.1.19 nat-pool

Creating Profiles

Use this (config-profile-default-rfs7000) instance to configure NAT pool commands.

```
rfs7000-37FABE(config-profile-default-rfs7000)#ip nat pool pool1 prefix-length

rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#ip nat pool pool1
prefix-length 1
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#?
Nat Policy Mode commands:
  address  Specify addresses for the nat pool
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal


rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)
```

Table 7.6 Summarizes nat-pool commands

Table 7.6 *nat-pool Commands*

Command	Description	Reference
address	Specifies addresses for the NAT pool	*page 7-52*
no	Negates a command or sets its default	*page 7-53*

7.1.19.1 address

nat-pool

Specifies IP addresses for the nat pool

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
address [<IP>|range]
address range <Start-IP> <End-IP>
```

Parameters

<IP>|range <Start-IP> <End-IP>]	• <IP> – Specifies a single IP address to add to the NAT pool
	• range – Specifies an address range to configure
	  • <Start-IP> – Specifies the starting IP address
	  • <End-IP> – Specifies the ending IP address

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#address range
172.16.10.2 172.16.10.8
```

7.1.19.2 no

nat-pool

Negates a comamnd or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no address
```

Parameters

None

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)#no address
```

7.1.20 interface

Creating Profiles

Selects an interface to configure

This command is used to enter the interface configuration mode for the specified physical controller *Virtual Interface* (SVI) interface. If the VLANx (SVI) interface does not exist, it's automatically created.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
interface [<WORD>|fe <1-4>|ge<1-8>|me1|port-channel<1-8>|radio <1-3>|up1|
   vlan<1-4094>|wwan1]
```

Parameters

<WORD>	Defines the name of the interface selected
fe <1-4>	Fast Ethernet interface
ge <1-8>	Gigabit Ethernet interface (4 for RFS7000 and 8 for RFS6000)
me1	Management interface **Note:** Not applicable for RFS4000
port-channel <1-8>	Select a port channel interface between 1 and 8
radio <1-3>	Select a radio between 1 and 3
up1	Uplink Gigabit Ethernet interface (RFS6000 and RFS7000 only)
vlan <1-4094>	Defines the VLAN interface
wwan1	Defines the wireless WAN interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#interface vlan 44
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#?
VLAN configuration commands:
 allow-management     Allow management
  crypto               Encryption module
  description          Vlan description
  dhcp-relay-incoming  Allow on-board DHCP server to respond to relayed DHCP
                       packets on this interface
  ip                   Interface Internet Protocol config commands
  no                   Negate a command or set its defaults
  shutdown             Shutdown the selected interface
  use                  Set setting to use

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

7.1.21 Interface Config Instance

Use the (config-profile-default-rfs7000) instance to configure the interfaces – Ethernet, VLAN and tunnel associated with the controller.

To switch to this mode, use the following command:

```
rfs7000-37FABE(config-profile-default-rfs7000)#interface [<interface-name>|fe<1-4>|ge <1-
4>|me1|port-channel <1-4>|radio|up1|vlan <1-4094>|wwan1]
rfs7000-37FABE(config-profile-default-rfs7000)# ge 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#?
Interface Config commands:

  cdp             Enable Cisco Discovery Protocol on port
  channel-group   Channel group commands
  description     Interface specific description
  dot1x           802.1X Authentication
  duplex          Set duplex to interface
  ip              Internet Protocol (IP)
  no              Negate a command or set its defaults
  power           PoE Command
  qos             Quality of service
  shutdown        Shutdown the selected interface
  spanning-tree   Spanning tree commands
  speed           Configure speed
  switchport      Set switching mode characteristics
  use             Set setting to use

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

Table 7.7 Summarizes the Interface Config Commands

Table 7.7 *Interface Config Commands*

Command	Description	Reference
cdp	Enables the *Cisco Discovery Protocol* (CDP) on ports	*page 7-58*
channel-group	Configures channel-group commands	*page 7-59*
description	Creates an interface specific description	*page 7-60*
dot1x	Configures 802.1X authentication settings	*page 7-61*
duplex	Specifies the duplex mode for the interface	*page 7-62*
ip	Sets the IP address for the assigned Fast Ethernet interface (ME), and VLAN Interface	*page 7-63*
lldp	Configures Link Local Discovery Protocol	*page 7-64*
no	Negates a command or sets its defaults	*page 7-65*

Table 7.7 *Interface Config Commands*

Command	***Description***	***Reference***
power	Invokes PoE commands to configure the PoE power limit and port priority	*page 7-66*
qos	Enables quality of service	*page 7-67*
shutdown	Disables the selected interface	*page 7-68*
spanning-tree	Configures spanning tree parameters	*page 7-69*
speed	Specifies the speed of a fast-ethernet (10/100) or a gigabit-ethernet port (10/100/1000)	*page 7-71*
switchport	Sets switching mode characteristics for a selected interface	*page 7-72*
use	Defines the settings to use with this command	*page 7-74*

7.1.21.1 cdp

Interface Config Instance

Enables the Cisco Discovery Protocol (CDP) on the controller ports

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
cdp [transmit|receive]
```

Parameters

[transmit|receive]	• receive – Enables snooping of CDP packets • transmit – Enables transmission of CDP packets

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#cdp transmit
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.2 channel-group

Interface Config Instance

Configures channel-group commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
channel-group <1-5>
```

Parameters

<1-5>	Specifies a group number for channel-group configuration

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#channel-group 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.3 description

Interface Config Instance

Creates an interface specific description

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
description [<LINE>|<WORD>]
```

Parameters

[<LINE>|<WORD>]	Defines the characters describing this interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#description "interface for
Retail King"
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.4 dot1x

Interface Config Instance

Configures 802.1X authentication settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dot1x [username <WORD>|password [0 <WORD>|2 <WORD>|<WORD>]
```

Parameters

[username <WORD>|password [0 <WORD> |2 <WORD>|<WORD>]	• usernname <WORD> – Sets the username for authentication
	• password [0|2|<WORD>] – Sets the password
	  • 0 – Enter a clear text password
	  • 2 – Enter an encrypted password
	  • <WORD> – Defines the password

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#dot1x username Bob password
motorola
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.5 duplex

Interface Config Instance

Specifies the duplex mode for the interface

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
duplex [auto|half|full]
```

Parameters

[auto|half|full]	• auto – Sets the ports duplexity automatically. The port automatically detects whether it should run in full or half-duplex mode • half – Sets the port to half-duplex mode • full – Sets the port to full-duplex mode

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#duplex auto
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.6 ip

Interface Config Instance

Sets the IP address for the assigned Fast Ethernet interface (ME), and VLAN interface

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip [arp|dhcp] trust
ip arp header-mismatch-validation
```

Parameters

[arp|dhcp]	• arp [header-mismatch-validation|trust] – Sets ARP for the packets
	  • header-mismatch-validation – Verifies the mismatch for source MAC address in ARP header and ethernet header
	  • trust – Sets the ARP trust state for ARP responses on this interface
	• dhcp trust – Uses a DHCP Client to obtain an IP address for the interface (this enables DHCP on a Layer 3 SVI)
	  • trust – Sets the DHCP trust state for DHXP responses on this interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#ip dhcp trust
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.7 lldp

Interface Config Instance

Configures Link Local Discovery Protocol

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
lldp [receive|transmit]
```

Parameters

[receive|transmit]	• receive – Enables snooping of LLDP PDUs • transmit – Enables transmimission of LLDP PDUs

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#lldp transmit
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.8 no

Interface Config Instance

Negates a command or sets its defaults

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [arp|cdp|channel-group|description|dot1k|duplex|ip|lldp|power|qos|
shutdown|spanning-tree|speed|switchport|use]
```

Parameters

None

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#no cdp
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#no duplex
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.9 power

Interface Config Instance

Invokes PoE commands to configure the PoE power limit and port priority. By default, the value for a GE port is set to low. Power is applied in order of priority, power overlaods are removed in the reverse order of priority.

Supported in the following platforms:

- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Switch Note: This command is not supported on the RFS7000 controller.

Syntax

```
power {limit <0-40>|prority}
power priority [critical|high|low]
```

Parameters

limit <0-40>	Sets the power limit on the given port to the stated power in Watts. Select the power limit value between 0-40 (Watts). It actually limits to 29.7W
priority [critical|high|low]	Sets PoE priority for port • critical – Sets the PoE priority as a critical priority • high – Sets the PoE priority as a high priority • low – Sets the PoE priority as a low priority

Usage Guidelines

Use `[no] power` to rollback the PoE configurations and set back the default configuration

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#power priority critical
% Error: No POE support on device type [rfs7000].
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.10 qos

Interface Config Instance

Enables *quality of service* (QoS)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
qos trust [802.1p|cos|dscp]
```

Parameters

trust [802.1p|cos|dscp]	Trust QoS values ingressing on interface • 802.1p – Sets the trust 802.1p COS values ingressing on the interface • cos – Sets the trust 802.1p COS values ingressing on the interface • dscp – Sets the trust IP DSCP QOS values ingressing on the interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#qos trust dscp
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.11 shutdown

Interface Config Instance

Disables the selected interface, the interface is administratively enabled unless explicitly disabled using this command.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
shutdown
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#shutdown
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.12 spanning-tree

Interface Config Instance

Configures spanning tree parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650

Syntax

```
spanning-tree [bpdufilter|bpduguard|edgeport|force-version <0-3>|
guard root|link-type|mst|port-cisco-interoperability |portfast]
spanning-tree [bpdufilter|bpduguard] [disable|enable]
spanning-tree link-type [point-to-point|shared]
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]
spanning-tree port-cisco-interoperability [disable|enable]
```

Parameters

bpdufilter [disable|enable]	Use this command to set a portfast BPDU filter for the port. Use the `no` parameter with this command to revert the port BPDU filter to its default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFast enabled ports do not transmit or receive BPDUs.
bpduguard [disable|enable]	Use this command to enable or disable the BPDU guard feature on a port. Use the `no` parameter with this command to set the BPDU guard feature to its default values. When the BPDU guard is set for a bridge, all portfast-enabled ports that have the BPDU-guard set to default shut down the port upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the `no shutdown` command), or by configuring the errdisable-timeout to enable the port after the specified interval.
edgeport	Enables an interface as an edge port
force-version <0-3>	Specifies the spanning-tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select from the following versions: • 0 – STP • 1 – Not supported • 2 – RSTP • 3 – MSTP The default value for forcing the version is MSTP

guard root	Enables the Root Guard feature for the port. The Root Guard disables the reception of superior BPDUs. The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state. Use the no parameter with this command to disable the Root Guard feature.
link-type [point-to-point|shared]	Enables or disables point-to-point or shared link types • point-to-point – Enables rapid transition • shared – Disables rapid transition
mst [<0-15> [cost <1-200000000>| port-priority <0-240>	Configures MST values on a spanning tree • <0-15> [cost <1-200000000>|port-priority <0-240>] – Defines the Instance ID • cost <1-200000000> – Defines the path cost for a port • port-priority <0-240> – Defines the port priority for a bridge
port-cisco-interoperability [disable|enable]	Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP). • enable – Enables CISCO Interoperability • disable – Disables CISCO Interoperability - The default value is disabled
portfast	Enables rapid transitions

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree bpdufilter
disable
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree bpduguard enable
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree force-version 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree guard root
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#spanning-tree mst 2 port-
priority 10
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#show context
 interface ge1
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1
  spanning-tree link-type shared
  spanning-tree bpduguard enable
  spanning-tree bpdufilter enable
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
  spanning-tree mst 2 cost 200
  qos trust 802.1p
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.13 speed

Interface Config Instance

Specifies the speed of a fast-ethernet (10/100) or a gigabit-ethernet port (10/100/1000)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650

Syntax

```
speed [10|100|1000|auto]
```

Parameters

10	Forces 10 Mbps operation
100	Forces 100 Mbps operation
1000	Forces 1000 Mbps operation
auto	Port automatically detects the speed it should run based on the port at the other end of the link. Auto negotiation is a requirement for using 1000BASE-T[3] according to the standard.

Usage Guidelines

Set the interface speed to auto detect and use the fastest speed available. Speed detection is based on connected network hardware

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#speed 10
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#speed auto
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.14 switchport

Interface Config Instance

Sets switching mode characteristics for the selected interface

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
switchport [access|mode|trunk]
switchport access vlan <1-4094>
switchport mode [access|trunk]
switchport trunk [allowed|native]
switchport trunk allowed vlan [<VLAN-ID>|add|none|remove]
switchport trunk allowed vlan [add|remove] <VLAN-ID>
switchport trunk native [tagged|vlan <1-4094>]
```

Parameters

access vlan <1-4094>	Configures the access VLAN of an access-mode port • vlan <1-4094> – Sets the VLAN when interface is in access mode
mode [access|trunk]	Sets the mode of the interface to access or trunk mode (can only be used on physical (layer2) interfaces) • access – If access mode is selected, the access VLAN is automatically set to vlan1. In this mode, only untagged packets in the access VLAN (vlan1) are accepted on this port. All tagged packets are discarded • trunk – If trunk mode is selected, tagged VLAN packets VLANs are accepted. The native vlan is automatically set to VLAN1. Untagged packets are placed in the native VLAN by the controller. Outgoing packets in the native VLAN are sent untagged. `trunk` is the default mode for both ports.

trunk [allowed |native]	Sets the trunking mode characteristics
	• allowed vlan – Configures trunk characteristics when the port is in trunk-mode
	  • vlan [add|none|remove] – Sets allowed VLANs
	  • none – Allows no VLANs to Xmit/Rx through the Layer2 interface
	  • add <vlan-id> – Adds VLANs to the current list
	  • remove <VLAN-ID> – Removes VLANs from the current list
	  • <VLAN-ID> – VLAN IDs added or removed. Can be either a range of VLAN (55-60) or list of comma separated IDs (35, 41 etc.)
	• native [tagged|vlan <1-4094>] – Configures the native VLAN ID of the trunk-mode port
	  • tagged – Tags the native VLAN
	  • vlan <1-4094> – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode

Usage Guidelines

Interfaces ge1-ge4 can be configured as trunk or in access mode. An interface (when configured as trunk) allows packets (from the given list of VLANs) to be added to the trunk. An interface configured as "*access*" allows packets only from native VLANs

Use the `[no] switchport (access|mode|trunk)` to undo switchport configurations

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#switchport trunk native tagged
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#

rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#switchport access vlan 1
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.21.15 use

Interface Config Instance

Defines the settings used with this command

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
use [ip-access-list in <IP-ACCESS-LIST>|mac-access-list in
<MAC-ACCESS-LIST>]
```

Parameters

ip-access-list in <IP-ACCESS-LIST>| mac-access-list in <MAC-ACCESS-LIST>]	• ip-access-list – Uses an IP access list
	  • in – Applies ACL on incoming packets
	  • <IP-ACCESS-LIST> – Specifies the IP access name to use with the list
	• mac-access-list – Uses a MAC access list
	  • in – Applies ACL on incoming packets
	  • <MAC-ACCESS-LIST> – Specifies the MAC access list name

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#use mac-access-list in test
rfs7000-37FABE(config-profile-default-rfs7000-if-ge1)#
```

7.1.22 Interface vlan Instance

Use the (config-profile-default-rfs7000) instance to configure interfaces – Ethernet, VLAN and the tunnel associated with the controller.

To switch to this mode, use the command:

```
rfs7000-37FABE(config-profile-default-rfs7000)#interface [<interface-name>|ge <1-4>|
me1|port-channel <1-4>|radio|up1|vlan <1-4094>]
rfs7000-37FABE(config-profile-default-rfs7000)#vlan 8
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

Table 7.8 Summarizes interface -vlan mode commands

Table 7.8 *interface-vlan commands*

Commands	Description	Reference
crypto	Defines the encryption module	*page 7-76*
description	Defines the VLAN description	*page 7-77*
dhcp-relay-incoming	Allows an on-board DHCP server to respond to relayed DHCP packets on this interface	*page 7-78*
ip	Configures Internet Protocol (IP) config commands	*page 7-79*
no	Negates a command or sets its default	*page 7-80*
shutdown	Shuts down the selected interface	*page 7-81*
use	Defines the settings used with this command	*page 7-82*

7.1.22.1 crypto

Interface vlan Instance

Sets the encryption module to use for this interface

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
crypto map <CRYPTO-MAP>
```

Parameters

map <CRYPTO-MAP>	Attaches a crypto map to the VLAN • <CRYPTO-MAP> – Specifies the map name

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#crypto map map1
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

7.1.22.2 description

Interface vlan Instance

Defines a description for the VLAN interface. Use this command to provide additional information about the VLAN.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
description <WORD>
```

Parameters

description <WORD>	Defines the VLAN description

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#description ”VLAN for the
sales team”
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#
```

7.1.22.3 dhcp-relay-incoming

Interface vlan Instance

Allows an on-board DHCP server to respond to relayed DHCP packets on this interface

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dhcp-relay-incoming
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#dhcp-relay-incoming
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan8)#
```

7.1.22.4 ip

Interface vlan Instance

Configures Internet Protocol (IP) config commands.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip [address|dhcp|helper-address <A.B.C.D>|nat]
ip address [<A.B.C.D/M> {secondary}|dhcp|zeroconfig {secondary} ]
ip nat [inside|outside]
ip dhcp client request options all
```

Parameters

address [<A.B.C.D/M> {secondary}|dhcp]	Sets the IP address of an interface • <A.B.C.D/M > – Specifies the IP address (e.g. 10.0.0.1/8) • secondary – Specifies a secondary IP address • dhcp – Uses a DHCP client to obtain an IP address for this interface
dhcp client request options all	Uses a DHCP client to configure the request • client – DHCP client • request – Configures the request • options – DHCP options • all – Configures all the DHCP options based on the request
helper-address <A.B.C.D>	Forwards DHCP and BOOTP packets • <A.B.C.D> – Specifies the IP for DHCP and BOOTP packet forwarding
nat [inside|outside]	Sets the *Network Address Translation* (NAT) of an interface • inside – Inside interface • outside – Outside interface

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#ip nat inside
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#

rfs7000-37FABE(config-profile-defalut-rfs7000-if-vlan2)#ip address 10.0.0.1/8
rfs7000-37FABE(config-profile-defalut-rfs7000-if-vlan2)#

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#ip helper-address
172.16.10.3
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan1)#ip dhcp client request
options all
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan1)#
```

7.1.22.5 no

Interface vlan Instance

Negate a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [crypto|description|ip|shut-down||use]
```

Parameters

crypto	Encryption module
description	Removes a VLAN description
dhcp-relay-monitoring	Prohibits an onboard DHCP server from responding to relayed DHCP packets on this interface
ip	Interface Internet Protocol config commands
shut-down	Re-enables the selected interface
use	Defines the stting used with this command

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#no use ip-access-list in
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#

rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#no allow-management
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#
```

7.1.22.6 shutdown

Interface vlan Instance

Shuts down the selected interface

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
shutdown
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#shutdown
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#
```

7.1.22.7 use

Interface vlan Instance

Defines the settings used with this command

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
use ip-access-list in <IP-ACCESS-LIST>
```

Parameters

ip-access-list in <IP-ACCESS-LIST>	Specifies the IP access list value • in – Sets incoming packets • IP-ACCESS-LIST – Specifies the IP access list name

Example

```
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#use ip-access-list in test
% Error: ip_acl[test] does not exist
rfs7000-37FABE(config-profile-default-rfs7000-if-vlan44)#
```

NOTE: The commands clrscr, commit, end, exit, help, revert, show, service are common across all chapters. For more information, see *Chapter 5, COMMON COMMANDS*.

7.1.23 led

Creating Profiles

Turns LEDs on/off on the access point

Supported in the following platforms:

- AP71xx
- AP650

Syntax

```
led
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#led
% Error: led configuration not available for this platform
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.24 legacy-auto-downgrade

Creating Profiles

Enables device firmware to auto downgrade when legacy devices are detected

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
legacy-auto-downgrade
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-defaullt)#legacy-auto-downgrade
rfs7000-37FABE(config-profile-defaullt)#
```

7.1.25 legacy-auto-update

Creating Profiles

Enables a legacy device firmware to be auto updated.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
legacy-auto-update {AP650|AP7131} image <FILE NAME>
```

Parameters

legacy-auto-update	Enables a legacy auto update

[AP650|AP7131] image <FILE>	• AP650 – Sets a legacy AP650 update firmware image
	• AP7131 – Sets a legacy AP7131 update firmware image
	  • image – Sets the path to the image
	  • <FILE> – Specifies the path and filename, e.g. flash:/ap.img

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#legacy-auto-update AP650 image
flash:/ap47d.img
rfs7000-37FABE(config-profile-default-rfs7000)#
rfs7000-37FABE(config-profile-defaultrfs7000)#legacy-auto-update
rfs7000-37FABE(config-profile-defaultrfs7000)#
```

7.1.26 lldp

Creating Profiles

Configures *Link Layer Discovery Protocol* (lldp)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
lldp [holdtime <10-1800>|med-tlv-select|run|timer <5-900>]
lldp med-tlv-select [inventory-management|power-management]
```

Parameters

holdtime <10-1800>	Sets the hold time value between <10-1800> in transmitted LLDP PDUs
med-tlv-select [inventory-management|power-management]	Media Endpoint Device TLVs • inventory-management – Enables inventory management discovery • power-management – Enables extended power via MDI discovery
run	Enables run link layer discovery protocol
timer <5-900>	Sets the timer for transmit interval between <5-900> seconds

Example

```
rfs4000-880DA7(config-profile-default-rfs4000)#lldp timer 20
rfs4000-880DA7(config-profile-default-rfs4000)#
```

7.1.27 load-balancing

Creating Profiles

Configures load balancing parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
load-balancing [ap-load-weightage|balance-ap-loads|balance-band-loads|balance-
channel-loads|band-ratio|client-weightage|equality-margin|hiwater-
threshold|throughput-weightage]
load-balancing [ap-load-weightage|client-weightage|throughput-weightage]
[2.4ghz|5ghz] <0-100>
load-balancing balance-channel-loads [2.4ghz|5ghz]
load-balancing band-ratio 2.4ghz <0-10> 5ghz <0-10>
load-balancing equality-margin [2.4ghz|5ghz|ap|band] <0-100>
load-balancing hiwater-threshold[ap|channel-2.4ghz|channel-5ghz] <0-100>]
```

Parameters

[ap-load-weightage |balance-ap-loads| balance-band-loads| balance-channel-loads| band-ratio|client-weightage| equality-margin| hiwater-threshold| throughput-weightage]	• ap-load-weightage [2.4ghz|5ghz] <0-100> – Configures weightage when calculating ap-load from radio loads • 2.4ghz – Weightage assigned to the 2.4ghz radio • 5ghz – Weightage assigned to the 5ghz radio • <0-100> – Sets weightage as a percentage from 0 to 100 • client-weightage [2.4ghz|5ghz] <0-100> – Configures weightage assigned to wireless client count • throughput-weightage [2.4ghz|5ghz] <0-100> – Configures weightage assigned to throughput • 2.4ghz – When calculating how much a 2.4GHz band/channel/radio is loaded • 5ghz – When calculating how much a 5GHz band/channel/radio is loaded • <0-100> – Sets weightage as a percentage from 0 to 100 • balance-channel-loads [2.4ghz|5ghz] – Enables balancing of channel loads amongst neighbors • 2.4ghz – Balance channel loads on 2.4ghz band • 5ghz – Balance channel loads on 5ghz band • band-ratio 2.4ghz <0-10> 5ghz <0-10> – Configures relative loading of 2.4ghz and 5ghz bands • 2.4ghz – Relative loading of 2.4ghz • 5ghz – Relative loading of 5ghz • <0-10> – Relative load in the ratio as a number between 0(no load) and 10 • equality-margin [2.4ghz|5ghz|ap|band] <0-100> – Configures maximum load difference that can be considered equal • ap – When comparing loads on different aps • band – When comparing loads on different bands • 2.4ghz|5ghz] <0-100> – When comparing loads on different 2.4ghz and 5ghz channels • <0-100> – Sets margin as a percentage of load between 1 and 100 • hiwater-threshold[ap|channel-2.4ghz|channel-5ghz] <0-100> – Configures the load beyond which the load balancing kicks in • [ap – For the ap's total load • channel-2.4ghz – For the ap's channel on 2.4ghz • channel-5ghz – For the ap's channel on 5ghz

Example

```
rfs4000-880DA7(config-profile-default-rfs4000)#load-balancing throughput-weightage 5
1
rfs4000-880DA7(config-profile-default-rfs4000)#

rfs4000-880DA7(config-profile-default-rfs4000)#load-balancing hiwater-threshold ap 1
rfs4000-880DA7(config-profile-default-rfs4000)#
rfs4000-880DA7(config-profile-default-rfs4000)#load-balancing balance-channel-loads
2.4ghz
rfs4000-880DA7(config-profile-default-rfs4000)#
```

7.1.28 local

Creating Profiles

Sets the username and password for local user authentication

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
local username <WORD> password <WORD>
```

Parameters

username <WORD> password <WORD>	• username <WORD> – Sets the username and password for local user authentication • password <WORD> – A string of 8 to 21 characters

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#local username Denvor password
symbol123
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.29 logging

Creating Profiles

Modifies message logging facilities

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
logging [aggregation-time <1-60>|buffered|console|facility|
forward|host||on|syslog]
logging [buffered|console|syslog] [<0-7>|alerts|
critical|debugging|emergencies|errors|informational|
notifications|warnings]
logging facility [local0|local1|local2|local3|
local4|local5|local6|local7]
logging host <IP>
logging forward on
```

Parameters

aggregation-time <1-60>	Sets the number of seconds for aggregating repeated messages. The value can be configured between 1-60 seconds.
buffered [<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications|warnings]	Sets the buffered logging level • <0-7> – Enter the logging severity level (0-7) • alerts – Set the immediate action needed, (severity=1) • critical – Critical conditions, (severity=2) • debugging – Debugging messages, (severity=7) • emergencies – System is unusable, (severity=0) • errors – Error conditions, (severity=3) • informational – Informational messages, (severity=6) • notifications – Normal but significant conditions, (severity=5) • warnings – Warning conditions, (severity=4)
console [<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications|warnings]	Sets the console logging level
forward on	Forwards system debug messages to controller or cluster members • on – Enables forwarding debug messages

facility [local0|local1| local2|local3|local4| local5|local6|local7]	Syslog facility in which log messages are sent • local0 – Syslog facility local0 • local1 – Syslog facility local1 • local2 – Syslog facility local2 • local3 – Syslog facility local3 • local4 – Syslog facility local4 • local5 – Syslog facility local5 • local6 – Syslog facility local6 • local7 – Syslog facility local7
host <IP>	Configures a remote host to receive log messages • <IP> – Remote host's IP address
on	Enables the logging of system messages
syslog [<0-7>|alerts| critical|debugging| emergencies|errors| informational| notifications|warnings]	Sets the syslog servers logging level

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#logging facility local4
rfs7000-37FABE(config-profile-default-rfs7000)#logging monitor notifications
```

7.1.30 mac-address-table

Creating Profiles

Configures the MAC address table

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mac-address-table [aging-time|static]
mac-address-table aging-time [0|<10-1000000>]
mac-address-table  <MAC-Address> <WORD> [<WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>]
```

Parameters

aging-time [0|<10-1000000>]	Sets the duration a learned MAC address persists after the last update • 0 – Disables aging • <10-1000000> – Sets the aging time in seconds
static <MAC-Address> <WORD> [WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>]	Static MAC address table entry • <MAC-Address> – Enter MAC address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF format • <WORD> – Specifies the VLAN name • <WORD> – Specifies the interface name • ge <1-4> – Specifies a GigabitEthernet interface value between 1 and 4 • me1 – Specifies the FastEthernet interface • pc <1-4> – Specifies a Port-Channel interface value between 1 and 4 • vlan <1-4094> – Specifies a VLAN index between 1 and 4094

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#mac-address-table static 00-40-96-B0-
BA-2A vlan1 ge 1
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.31 mint

Creating Profiles

Configures MiNT protocol commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mint [dis||level|link|mlcp|spf-latency]
mint dispriority-adjustment <-255-255>
mint level [leve11|leve2] area-id <1-4294967295>
mint link [ip|listen|vlan]
mint link listen ip <A.B.C.D> {adjacency-hold-time <2-600>|cost
<1-10000>|hello-interval <1-120>|level [1|2]}
mint link [ip <A.B.C.D>|vlan <1-4095>] > {adjacency-hold-time <2-600>|cost <1-
10000>|hello-interval <1-120>|level [1||2]}
mint mlcp [l2|l3]
mint spf-latency <0-60>
```

Parameters

dis[priority-adjustment <-255-255>|scatter]	Sets the relative priority for the router to become DIS • priority-adjustment <-255-255> – Sets adjustment added to base priority • <-255-255> – Priority adjustment value, added to fixed the base priority. Higher numbers result in higher priorities.
level [leve1|leve2] area-id <1-4294967295>	Configures MiNT routing levels • leve1 – Configures local MiNT routing • leve2 – Configures inter-site MiNT routing The following parameters are common for the above: • area-id – Specifies a routing area identifier • <1-4294967295> – Specifies an area identifier value

link [ip <A.B.C.D>|listen||vlan <1-4095>] <A.B.C.D> {adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|level [1|2]}	Creates a MiNT routing link
	• ip <A.B.C.D> – Creates a MiNT tunnel over UDP/IP
	  • <A.B.C.D> – Specifies a peer IP address
	• listen<A.B.C.D> – Creates listening link over UDP/IP
	  • <A.B.C.D> – Specifies a listening IP address
	• vlan <1-4095> – Enables MiNT routing on a VLAN
	  • <1-4095> – Specifies a VLAN index value
	The following parametrs are common for all the above:
	  • adjacency-hold-time <2-600> – Adjacency lifetime after hello packets cease
	  • <2-600> – Specifies the lifetime in seconds
	  • cost <1-10000> – Specifies the link cost
	  • <1-10000> – Specifies the cost in arbitrary units
	  • hello-interval <1-120> – Hello packet interval
	  • <1-120> – Specifies the number of seconds between hello packets
	  • level[1|2] – Specifies existing routing levels
	  • 1 – Level 1 only (local)
	  • 2 – Level 2 only (inter-site)

mlcp [l2|l3]	Configures the MINT link creation protocol • l2 – MLCP over Layer 2 (VLAN) links • l3 – MLCP over Layer 3 (IP) links
spf-latency <0-60>	Latency of SPF routing recalculation • <0-60> – Specifies the latency in seconds

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#mint level 1 area-id 88
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#mint link ip 1.2.3.4 level 1
rfs7000-37FABE(config-profile-default-rfs7000)#


rfs7000-37FABE(config-profile-default-rfs7000)#show mint links
 vlan-1 : level 1, cost 10, 1 adjacencies, DIS 70.37.fa.be (self)
rfs7000-37FABE(config-profile-default-rfs7000)#show mint stats
1 L1 neighbors
L1 LSP DB size 2 LSPs (1 KB)
2 L1 routes
Last SPFs took 0s
SPF (re)calculated 6 times.
levels 1
base priority 180
dis priority 180
rfs7000-37FABE(config-profile-default-rfs7000)#show mint route
Destination : Next-Hop(s)
00.00.00.00 :  00.00.00.00
70.88.9e.c4 :  70.88.9E.C4
70.37.fa.be :  70.37.FA.BE
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.32 misconfiguration-recovery-time

Creating Profiles

Verifies controller connectivity after the configuration is received

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
misconfiguration-recovery-time <60-300>
```

Parameters

<60-300>	Sets the recovery time between 60 and 300 seconds

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#misconfiguration-recovery-time 65
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.33 monitor

Creating Profiles

Enables critical resource monitoring

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
monitor <A.B.C.D> ping-mode [arp-icmp|arp-only vlan <1-4094>]
```

Parameters

<A.B.C.D> ping-mode [arp-icmp|arp-only vlan <1-4094>]	Specify the critical resource IP address to be monitored • ping-mode [arp-icmp|arp-only vlan <1-4094>] – Specify the protocol to be used to ping the critical resource • arp-only – Uses either arp requests or icmp echo request to monitor critical resource (requires the AP/Controller to have an IP address) • arp-only vlan <1-4094> – Uses only probing arp requests to monitor critical resource (suitable for AP/Controller without IP address) • vlan <1-4094> – Specify the VLAN on which the probing arp requests have to be sent • <1-4094> – Specify the VLAN ID

Example

```
rfs4000-880DA7(config-critical-resource-policy-testpolicy)#monitor 172.16.10.112
ping-mode arp-only vlan 1
rfs4000-880DA7(config-critical-resource-policy-testpolicy)#

rfs4000-880DA7(config-critical-resource-policy-testpolicy)#monitor 172.16.10.112
 ping-mode arp-icmp
rfs4000-880DA7(config-critical-resource-policy-testpolicy)#

rfs4000-880DA7(config-critical-resource-policy-testpolicy)#show context
critical-resource-policy testpolicy
 monitor 172.16.10.112 ping-mode arp-only vlan 1
rfs4000-880DA7(config-critical-resource-policy-testpolicy)#
```

7.1.34 neighbor-inactivity-timeout

Creating Profiles

Configures neighbor inactivity timeout factor

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
neighbour-inactivity-timeout <1-1000
```

Parameters

<1-1000>	<1-1000> – Sets a timeout period, in seconds, for the neighbor-inactivity factor. The value can be anything between 1 to 1000 seconds

Example

```
rfs7000-37FABE(config-profile-defaullt)#neighbor-inactivity-timeout 500
rfs7000-37FABE(config-profile-defaullt)#
```

7.1.35 neighbor-info-interval

Creating Profiles

Configures neighbor information exchange interval

Supported in the following platforms:

- RFS7000
- RFS6000
- RF4000
- AP7131
- AP650
- AP6511
- AP6532

Syntax

```
neighbor-info-interval <1-100>
```

Parameters

<1-100>	Set interval in seconds as a number from 1 to 100

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#neighbor-info-interval 6
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.36 no

Creating Profiles

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [aaa|arp|autoinstall|ap-upgrade|automatic-write|bridge|cdp|
cluster|controller|controller-group|crypto|domain-lookup
|dscp-mapping|events|hb-holdtime|hb-interval|interface|ip|
legacy-auto-update|logging|local|mac-address-table|mint|name-server|
ntppreferred-controller-group||radius|rf-domain-manager|spanning-tree|use|
wep-shared-key-auth|service]
```

Parameters

None

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#no cluster
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.37 noc

Creating Profiles

Configurse the noc related settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
noc update-interval  [<5-3600>|auto]
```

Parameters

update-interval [<5-3600>|auto]	Configures the noc statistics update interval • <5-3600> – Specify the update interval between 5 and 3600 seconds • auto – Noc statistics update interval is automatically adjusted by the Controller based on the load

Example

```
rfs4000-880DA7(config-profile-default-rfs4000)#noc update-interval 25
rfs4000-880DA7(config-profile-default-rfs4000)#
```

7.1.38 ntp

Creating Profiles

Configure *Network Time Protocol* (NTP) values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ntp server <A.B.C.D> {autokey|key|prefer|version}
ntp server  <A.B.C.D> autokey {prefer version <1-4>|version <1-4>}
ntp server  <A.B.C.D> key md5 [0 <WORD>|2<WORD>|<WORD>]{prefer version
<1-4>|version <1-4>}
ntp server  <A.B.C.D> prefer version <1-4>
ntp server  <A.B.C.D> version <1-4> {prefer}
```

Parameters

server <A.B.C.D>	Configures a NTP server • <A.B.C.D> – Configures an IP address for the server • autokey {prefer version <1-4>|version <1-4>} – Configures an autokey peer authentication scheme • key md5 [0 <WORD> <WORD>|2|<WORD>] {prefer version <1-4>|version <1-4>} – Defines the authentication key for trusted time sources • md5 [0 <WORD> |2 <WORD>|<WORD>] – Sets MD5 authentication • 0 – Password is specified unencrypted • 2 – Password is specified encrypted with password encryption secret • < WORD> – Sets an authentication key • prefer version <1-4> – Optional. Prefers this peer when possible. • version <1-4> {prefer} – Optional. Configures the NTP version

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#ntp server 172.16.10.10
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#ntp server 172.16.10.1 version 1
prefer
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#ntp server 172.16.10.9 key md5 0
sharedkey1 prefer version 1
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.39 preferred-controller-group

Creating Profiles

Specifies the controller group the system prefers for adoption

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
preferred-controller-group <WORD>
```

Parameters

<WORD>	Specifies the controller group name the system prefers for adoption

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#preferred-controller-group testgroup1
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.40 power-config

Creating Profiles

Configures the power mode feature

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
power-config [af-option|at-option||mode]
power-config af-option[range|throughput]
power-config at-option [range|throughput]
power-config mode [auto|3af]
```

Parameters

af-option [range|throughput]	Configures the af power option mode • range – Configures the af power range mode • throughput – Configures the power throughput mode
at-option [range|throughput]	Configures the af power option mode • range – Configures the af power range mode • throughput – Configures the power throughput mode
mode [auto|3af]	Configures the power mode of this AP • 3af – Forces an AP bring up at the 3af power mode • auto – Power the detection auto mode

Example

```
rfs7000-37FABE(config-profile-defalut-rfs7000)#power-config af-option range
% Warning: AP must be restarted for power-management change to take effect.
rfs7000-37FABE(config-profile-defalut-rfs7000)#
rfs7000-37FABE(config-profile-defalut-rfs7000)#power-config at-option throughput

% Warning: AP must be restarted for power-management change to take effect.
rfs7000-37FABE(config-profile-defalut-rfs7000)#
```

7.1.41 radius

Creating Profiles

Configures device-level RADIUS authentication parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
radius [nas-identifier|nas-port-id] <WORD>
```

Parameters

nas-identifier <WORD>	Specifies the RADIUS NAS Identifier attribute tused by a device • <WORD> – Specifies the NAS identifier
nas-port-id<WORD>	Specifies the RADIUS NAS port ID attribute tused by a device • <WORD> – Specifies the NAS port ID

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#radius nas-port-id 1
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#radius nas-identifier test
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.42 rf-domain-manager

Creating Profiles

Enables the RF Domain manager feature

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rf-domain-manager [capable|priority <1-10000>]
```

Parameters

capable	Enables a device to become site manager
priority <1-10000>	Assigns a priority vlaue for site manager selection • <1-10000> – Select a priority value

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#rf-domain-manager priority 9
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#rf-domain-manager capable
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.43 service

Creating Profiles

Service Commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
service [watchdog|show cli]
```

Parameters

[watchdog|show cli]	• watchdog – Enables the watchdog • show cli – Displays running system information

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#service watchdog
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.44 spanning-tree

Creating Profiles

Enables spanning tree commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
spanning-tree [errdisable|mst|portfast]
spanning-tree errdisable recovery [cause bpduguard|interval
<10-1000000>]
spanning-tree mst [<0-15> priority  <0-61440>|cisco-interoperability [enable|disable]
|enable|forward-time <4-30> |hello-time
<1-10>|instance <1-15>|max-age <4-60> |max-hops  <7-127>|region <LINE>|revision <0-
255>]
spanning-tree portfast [bpdufilter| bpduguard] default
```

Parameters

errdisable recovery [cause bpduguard |interval <10-1000000>]	• Disables error • recovery – Enables the timeout mechanism for a port to be recovered • cause bpduguard – Specifies the reason for errdisable • bpduguard – Recovers from errdisable due to bpduguard • interval <10-1000000> – Specifies the interval after which a port is enabled • <10-1000000> – Specifies an errdisable-timeout interval in seconds.

mst [<0-15> priority <0-61440>| cisco-interoperability [enable|disable] |enable| forward-time <4-30> |hello-time <1-10>|instance <1-15>|max-age <4-60> | max-hops <7-127>|region <LINE>|revision <0-255>]	Configures multiple spanning tree commands
	• <0-15> – Specifies the number of instances required for configuration
	  • priority <0-61440> – Sets the bridge priority for an instance to the value specified. Use the no parameter with this command to restore the default bridge priority value
	  • <0-61440> – Bridge priority in increments of 4096 (Lower priority indicates greater likelihood of becoming root)
	• cisco-interoperability [enable|disable] – Enables/disables CISCO interoperability
	• Enable – Enables the multiple spanning tree protocol
	• forward-time <4-30> – Specifies the forwarding delay time in seconds between 4 -30
	• hello-time <1-10> – Specifies the hello BDPU interval in seconds within the range 1-10
	• Instance <1-15> – Defines the instance ID to which the VLAN is associated
	• max-age <4-60> – Maximum time to listen for the root bridge in seconds. Enter a value between 4 and 60
	• max-hop <7-127> – Maximum hops when BPDU is valid
	• region <LINE> – MST region
	• revision <0-255> – Sets the revision number of the MST bridge.
	  • <0-255> – Defines the revision number for configuration information

portfast [bpdufilter| bpduguard] default	Enables the portfast feature on a bridge • bpdufilter default – Use the bpdu-filter command to set the BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter value to the default value. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures PortFast enabled ports do not transmit or receive BPDUs • bpduguard default – Guards portfast ports against BPDU receive • default – Enables the BPDU filter on portfast enabled ports by default

Usage Guidelines

If a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

Generally, spanning tree configuration settings in the config mode define the configuration for bridge and bridge instances.

MSTP works based on instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances.

Controllers with the same instance, VLAN mapping, revision number and region names define a unique region. Controllers in the same region exchange bridge protocol data units (BPDUs) with instance record information within.

Example

```
rfs7000-37FABE(config-profile-defaultrfs7000)#spanning-tree errdisable recovery
cause bpduguard
rfs7000-37FABE(config-profile-defaultrfs7000)#
rfs7000-37FABE(config-profile-defaultrfs7000)#spanning-tree mst 1 priority 4096
rfs7000-37FABE(config-profile-defaultrfs7000)#
rfs7000-37FABE(config-profile-defaultrfs7000)#spanning-tree portfast bpdufilter
default
rfs7000-37FABE(config-profile-defaultrfs7000)#
```

7.1.45 use

Creating Profiles

Defines the settings used with this command

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax Profiles

```
use [adoption-policy|advanced-wips-policy|
captive-portal|critical-resource-policy||dhcp-server-policy|event-system-
policy|firewall-policy|igmp-snoop-policy| management-policy|
radius-server-policy|role-policy]
```

Syntax Device Mode

```
use [adoption-policy|advanced-wips-policy|
captive-portal|critical-resource-policy||dhcp-server-policy|
firewall-policy|igmp-snoop-policy|management-policy|profile|
radius-server-policy|rf-domain|role-policy|
smart-rf-policy|trustpoint|wips-policy]
```

NOTE: The Parameter Table contains the 'use' command parameters for the Profiles and Device modes.

Parameters

use [adoption-policy| advanced-wips-policy| captive-portal| critical-resource-policy| dhcp-server-policy| firewall-policy| igmp-snoop-policy| management-policy|profile| radius-server-policy| rf-domain|role-policy| smart-rf-policy| trustpoint|wips-policy]	Uses the policies as defined • adoption-policy – Sets an adoption policy • advanced-wips-policy – Creates/configures an advanced-wips policy • captive-portal – Captive portal access configuration • critical-resource-policy – Sets a critical resource policy • dhcp-server-policy – Sets a DHCP server policy • event-system-policy – Sets an event system policy • firewall-policy – Sets the firewall policy • igmp-snoop-policy – Sets an IGMP snoop policy • management-policy – Sets a management policy • radius-server-policy – Sets a device's onboard RADIUS policy • rf-domain – Specify the RF-Domain from which the connected device receives its configuration • role-policy – Sets a role policy configuraion • smart-rf-policy – Configures the smart-rf policy • trustpoint <WORD> – Uses a trustpoint for the service • https – Uses the trustpoint for HTTPS • radius-ca-certificate – Uses the trustpoint as a certificate authority, for validating client certificates using EAP • radius-server-certificate – Uses the trustpoint for a RADIUS server certificate • wips-policy – Configures the WIPS policy

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#use role-policy test
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#use adoption-policy test
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#use trustpoint trust1 https radius-
ca-certificate radius-server-certificate
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.1.46 vpn

Creating Profiles

Configures VPN settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
vpn authentication-method [local|radius]
```

Parameters

authentication-method [local|radius]	Selects an authentication scheme • local – Used for user based authentication • radius – Used for RADIUS server authentication

Usage Guidelines

Virtual Private Network (VPN) enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt information at the IP level.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#vpn authentication-method local
rfs7000-37FABE(config-profile-default-rfs7000)#

rfs7000-37FABE(config-profile-default-rfs7000)#vpn authentication-method  radius
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.1.47 wep-shared-key-auth

Creating Profiles

Enables support for 802.11 WEP shared key authentication

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wep-shared-key-auth
```

Parameters

None

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#wep-shared-key-auth
rfs7000-37FABE(config-profile-default-rfs7000)#
```

7.2 Device Specific Commands

Use the (config) instance to configure device specific parameters.

To navigate to this instance, use the following commands:

```
rfs7000-37FABE(config)#ap7131?
rfs7000-37FABE(config)#ap7131 00-15-70-88-9E-C4
```

rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#

Table 7.9 Summarizes Device Mode commands

Table 7.9 *Device Mode Commands*

Command	Description	Reference
ap-upgrade	Upgrades AP firmware	*page 7-117*
area	Sets the name of area where the system is located	*page 7-118*
contact	Sets contact information	*page 7-119*
country-code	Configures the controller country code	*page 7-120*
dhcp-redundancy	Enables DHCP redundancy	*page 7-121*
floor	Sets the name of a floor within a building where the system is deployed	*page 7-122*
hostname	Sets a system's network name	*page 7-123*
layout-coordinates	Configures layout coordinates	*page 7-124*
location	Configures the location the system is deployed	*page 7-125*
mac-name	Configures MAC name to name mappings	*page 7-126*
neighbor-info-interval	Configures the neighbor information exchange interval	*page 7-127*
override-wlan	Configures RF Domain level overrides for a WLAN	*page 7-128*
remove-override	Removes overrides from a device	*page 7-129*
rsa-key	Assigns a RSA key to SSH	*page 7-130*
sensor-server	Configures a AirDefense sensor server	*page 7-131*
stats	Configures statistics stettings	*page 7-132*
timezone	Configures controller timezone settings	*page 7-133*

Table 7.9 *Device Mode Commands*

Command	Description	Reference
trustpoint	Assigns a trustpoint to a service	*page 7-134*
wwan	Configures wireless WAN parameters	*page 7-135*

7.2.1 ap-upgrade

Device Specific Commands

Upgrades access point firmware to the latest version

Supported in the following platforms:

- AP71xx
- AP650

Syntax

```
ap-upgrade [all|ap650|ap7131]
ap-upgrade [ap650|ap7131] <MAC>
```

Parameters

[all|ap650|ap7131]	• all – Upgrades all access points
	• ap650 <MAC> – Upgrades an AP650 device
	  • DEVICE-AP650 – MAC address of a AP650 device
	• ap7131 – Upgrades an AP7131 device
	  • DEVICE-AP7131 – MAC address of a AP7131 device

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#ap-upgrade all
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.2 area

Device Specific Commands

Sets the name of area where the system is located

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
area <WORD>
```

Parameters

area <WORD>	Sets the name of area where the system is located

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#area RMZEcoSpace
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.3 contact

Device Specific Commands

Defines a contact for a deployed devices

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
contact <WORD>
```

Parameters

contact <WORD>	Enter a name to define the contact

Example

```
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#contact symbol
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#
```

7.2.4 country-code

Device Specific Commands

Sets the country of operation. All existing radio configurations are erased.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
country-code <WORD>
```

Parameters

`country-code <WORD>`	Configures the device to operate in a defined country. <country-code> is the 2 letter ISO-3166 country code

Example

```
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#country-code us
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#
```

7.2.5 dhcp-redundancy

Device Specific Commands

Enables DHCP redundancy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dhcp-redundancy
```

Parameters

None

Example

```
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#dhcp-redundancy
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#
```

7.2.6 floor

Device Specific Commands

Sets the name of a floor within a building where the system is located

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
floor <WORD>
```

Parameters

<WORD>	Sets the name of a floor within a building where the system is located

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#floor 5floor
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.7 hostname

Device Specific Commands

Sets system's network name

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
hostname <WORD>
```

Parameters

hostname <WORD>	Sets the name of the controller. This name is displayed when the controller is accessed from any network.

Example

```
rfs7000-37FABE(config-device-00-15-70-88-9E-C4)#hostname myrfs7000
```

7.2.8 layout-coordinates

Device Specific Commands

Configures layout coordinates for the device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
layout-coordinates  <0.0-4096.0>  <0.0-4096.0>
```

Parameters

<0.0-4096.0> <0.0-4096.0>	• <0.0-4096.0> – Specify X coordinate between 0 and 4096.0 • <0.0-4096.0> – Specify Y coordinate between 0 and 4096.0

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#layout-coordinates 1.5 2
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#

rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#show context
rfs7000 00-15-70-37-FA-BE
 use profile Profile_7K_TechPubs
 use rf-domain RFDOMAIN_TechPubs
 hostname rfs7000-37FABE
 layout-coordinates 1.5 2.0
 license AP
8088bb045018988b85bc057b560ab7edbc68029885fbcc680a96194dfbeedc28d4117058eb53bd8b
 license AAP
8088bb045018988b5985f7127ca1d354bc68029885fbcc68b6025fb695384946d4117058eb53bd8b
 autoinstall configuration
 autoinstall firmware
 use dhcp-server-policy DHCP_POLICY_TechPubs
 logging on
 logging console warnings
 logging buffered warnings
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.9 location

Device Specific Commands

Configures the location where a controller managed device is deployed

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
location <WORD>
```

Parameters

<WORD>	Configures the location where the device is deployed within a building

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#location SarjapurRingRoad
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#show context
rfs7000 00-15-70-37-FA-BE
 use profile default-rfs7000
 use rf-domain default
 hostname rfs7000-37FABE
 building RMZEcospace
 floor 5floor
 location SarjapurRingRoad
```

7.2.10 mac-name

Device Specific Commands

Configures a MAC name for mappings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mac-name <AA-BB-CC-DD-EE-FF> <WORD>
```

Parameters

<AA-BB-CC-DD-EE-FF> <WORD>	Configures a MAC address • <WORD> – Specifies the 'friendly' name used for this MAC address in events and statistics

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#mac-name 11-22-33-44-55-66
testrfs7000
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#commit
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#show context

rfs7000 00-15-70-37-FA-BE
 use profile default-rfs7000
 use rf-domain default
 hostname rfs7000-37FABE
 mac-name 11-22-33-44-55-66 testrfs7000
 interface me1
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface ge2
 interface ge3
 interface ge4
 interface vlan1
  ip address 172.16.10.2/24
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.11 neighbor-info-interval

Device Specific Commands

Configures the neighbor information exchange interval

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
neighbor-info-interval <1-100>
```

Parameters

neighbor-info-interval <1-100>	Sets the neighbor information exchange interval between 1 to 100 seconds

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#neighbor-info-interval 10
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.12 override-wlan

Device Specific Commands

Configures RF Domain level overrides for a WLAN

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
override-wlan WLAN [ssid <WORD>|vlan-pool <1-4094> {limit} <0-8192>|
wpa-wpa2-psk <WORD>]
```

Parameters

WLAN [ssid <WORD>|vlan-pool <1-4094>|wpa-wpa2-psk <WORD>]	Enter the name of the WLAN to be configured
	• ssid <WORD> – Configures the SSID for this WLAN
	  • <WORD> – Specifies a case-sensitive alphanumeric SSID
	• vlan-pool <1-4094> {limit} – Configures a pool of VLANs for the WLAN
	  • <1-4094> – Specifies a VLAN ID between 1 and 4094
	  • {limit <0-8192>} – Specifies a value between 0 and 8192 to limit the number of users on this VLAN
	• wpa-wpa2-psk <WORD> – Configures the WPA-WPA2 key or passphrase for the WLAN

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#override-wlan test vlan-pool 8 limit
9
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#commit
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#show context

rfs7000 00-15-70-37-FA-BE
 use profile default-rfs7000
 use rf-domain default
 hostname rfs7000-37FABE
 override-wlan test vlan-pool 8 limit 9
 mac-name 11-22-33-44-55-66 testrfs7000
 interface me1
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface ge2
 interface ge3
 interface ge4
 interface vlan1
  ip address 172.16.10.2/24
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.13 remove-override

Device Specific Commands

Removes overrides from a device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
remove-override <parameters>
```

Parameters

None

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#remove-override ?
  all                 Remove all overrides for the device
  arp                 Static Address Resolution Protocol (ARP)
  autoinstall         Autoinstall Configuration commands
  bridge              Bridge group commands
  cluster             Cluster configuration
  contact             The contact
  country-code        The country of operation
  dhcp-redundancy     DHCP redundancy
  domain-lookup       Domain lookup
  dscp-mapping        IP DSCP to 802.1p priority mapping for untagged frames
  events              System event messages
  firewall            Enable/Disable firewall
  global              Remove global overrides for the device but keeps
                      per-interface overrides
  hb-holdtime         Hold time
  hb-interval         Heartbeat interval
  interface           Select an interface to configure
  ip                  Internet Protocol (IP)
  location            The location
              Modify message logging facilities
  mac-address-table   MAC Address Table
  name-server         Name server
  ntp                 Configure NTP
  override-wlan       Overrides for wlans
  power-config        Configure power mode
  rf-domain-manager   RF Domain Manager
  sensor-server       Motorola AirDefense WIPS sensor server configuration
  timezone            The timezone
  use                 Set setting to use
  service             Service Commands
```

7.2.14 rsa-key

Device Specific Commands

Assigns a RSA key to a service

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rsa-key ssh <WORD>
```

Parameters

ssh <WORD>	Assigns the RSA key to SSH • <WORD> – Specifies the RSA key name. This should be installed on the device using PKI commands in enable mode

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#rsa-key ssh rsa-key1
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.15 sensor-server

Device Specific Commands

Configures a Motorola Solutions AirDefense sensor server

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
sensor-server <1-3> ip <A.B.C.D> {port}[443|8443|<1-65535>]
```

Parameters

<1-3> ip <A.B.C.D> {port} <1-65535>	<1-3> – Select a server to configure with an IP address and optional port number • ip <A.B.C.D> – Configures the IP address of the server • {port} [443|8443|<1-65535>] – Specifies port value • 443 – The default port used by AirDefense Server • 8443 – The default port used by Advanced-WIPS on a controller • <1-65535> – Manually sets the port number of the Advanced-WIPS/AirDefense server

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#sensor-server 2 ip 172.16.10.7 port
1080
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#

rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#show context
rfs7000 00-15-70-37-FA-BE
 use profile default-rfs7000
 use rf-domain default
 hostname rfs7000-37FABE
 timezone india
 sensor-server 2 ip 172.16.10.7 port 1080
 interface me1
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface ge2
 interface ge3
 interface ge4
 interface vlan1
  ip address 172.16.10.2/24
 interface vlan4
  ip address 157.235.208.252/24
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.16 stats

Device Specific Commands

Configures the statistics related stettings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
stats open-window <1-2> {sample-interval <5-86640>} {size <3-100>}
```

Parameters

open-window <1-2> {sample-interval <5-86640>} {size <3-100>}	Opens a stats-window to fetch trending data. Set the index value between 1 and 2 • {sample-interval <5-86640>} – Sets the sample interval value between 5 and 86640 seconds • {size <3-100>} – Sets the stats window size and number of samples collected

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#stats open-window 1 sample-interval
77 size 10
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.17 timezone

Device Specific Commands

Configures controller timezone settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
timezone <timezone>
```

Parameters

timezone <timezone>	Configures the controller timezone settings

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#timezone india
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.18 trustpoint

Device Specific Commands

Assigns a trustpoint to a service

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
trustpoint [https|radius-ca|radius-server] <WORD>
```

Parameters

[https|radius-ca|radius-server] <WORD>	• https <WORD> – Assigns the trustpoint to HTTPS • radius-ca <WORD> – Assigns the trustpoint as a certificate authority for validating client certificates using EAP • radius-server <WORD> – Assigns the trustpoint for a RADIUS server certificate • <WORD> – Specifies the trustpoint name. This should be installed on the device using PKI commands in enable mode

Example

```
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#trustpoint radius-ca trust2
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

7.2.19 wwan

Device Specific Commands

Configures Wireless WAN interface parameters

Supported in the following platforms:

- RFS4000
- RFS6000

Syntax

```
wwan [apn <WORD>|auth-type|crypto-map <CRYPTo-MAP>|enable|ip
|password|username <WORD>]
wwan auth-type [chap|mschap|mschap-v2|pap]
wwan ip nat [inside|outside]
wwan password [2|<WORD>]
```

Parameters

apn <WORD>	Enter the access point name provided by the service provider • <WORD> – A string of up to 25 characters
auth-type [chap|mschap|mschap-v2|pap]	Specify the authentication-type from the following: • chap – Challenge Handshake Authentication Protocol • mschap – Microsoft CHAP extensions • mschap-v2 – Microsoft CHAP extensions Version 2 • pap – Password Authentication Protocol
crypto-map <CRYPTO-MAP>	Enter a crypto map for wireless WAN • <CRYPTo-MAP> – A string of up to 256 characters
enable	Enable wireless WAN feature

ip nat [inside|outside]	Configures Internet Protocol (IP) settings
	• nat [inside|outside] – Specifies *Network Address Translation* (NAT) information
	  • inside – Marks wireless WAN as NAT inside interface
	  • outside – Marks wireless WAN as NAT outside interface

username <WORD>	Enter the username provided by the service provider • <WORD> – A string of up to 32 characters
password <WORD>	Enter the password provided by the service provider • 2 – Enter encrypted password • <WORD> – A string of up to 30 characters

Example

```
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#wwan enable
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#

rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#wwan username testuser
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#

rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#wwan password mototest
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#
```

CHAPTER 8 AAA-POLICY

This chapter summarizes the aaa-policy commands within the CLI structure.

Use the (config) instance to configure aaa-policy related configuration commands. To navigate to the config-aaa-policy instance, use the following commands:

```
rfs7000-37FABE(config)#aaa-policy <policy-name>
rfs7000-37FABE(config-aaa-policy-test)#?
AAA Policy Mode commands:
  accounting           Configure accounting parameters
  authentication       Configure authentication parameters
  health-check         Configure server health-check parameters
  mac-address-format   Configure the format in which the MAC address must be
                       filled in the Radius-Request frames
  no                   Negate a command or set its defaults
  server-pooling-mode  Configure the method of selecting a server from the
                       pool of configured AAA servers
  use                  Set setting to use

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-aaa-policy-test)#


rfs7000-37FABE(config-aaa-policy-test)#
```

8.1 aaa-policy

Table 8.1 Summarizes aaa-policy commands

Table 8.1 *aaa-policy Commands*

Command	Description	Reference
accounting	Configures accounting parameters	*page 8-3*
authentication	Configures authentication parameters	*page 8-7*
clrscr	Clears the display screen	*page 8-15*
commit	Commits (saves) the changes made in the current session	*page 8-18*
do	Runs commands from EXEC mode	*page 8-19*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 8-21*
exit	Ends the current mode and moves to the previous mode	*page 8-22*
health-check	Configures health check parameters	*page 8-23*
help	Displays the interactive help system	*page 8-24*
mac-address-format	Configures the format the MAC addresses must be filled	*page 8-11*
no	Negates a command or sets its default	*page 8-12*
revert	Reverts the changes to their last saved configuration	*page 8-25*
server-pooling-mode	Defines the method for selecting a server from the pool of configured AAA servers	*page 8-13*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 8-26*
show	Displays running system information	*show*
use	Defines the settings used for AAA commands	*page 8-14*
write	Writes information to memory or terminal	*page 8-15*

8.1.1 accounting

aaa-policy

Configures accounting parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
accounting [interim|server|type]
accounting interim  interval <60-3600>

accounting server [<1-6>|preference]
accounting server <1-6> [dscp <0-63>|host |nai-routing|onboard|
proxy-mode|retry-timeout-factor <50-200>|timeout]
accounting server <1-6> host <WORD> secret [0 <WORD>|2 <WORD>|<WORD>] {port} <1-65535>
accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <WORD> {strip}
accounting server <1-6> onboard [self|controller]
accounting server <1-6> proxy-mode [none|through-controller|
through-rf-domain-manager]
accounting server <1-6> timeout <1-60> {attempts} <1-10>
accounting server preference [auth-server-host|auth-server-number|none

accounting type [start-interim-stop|start-stop|stop-only]]
```

Parameters

interim interval <60-3600>	Configures interim accounting parameters • interval <60-3600> – Configures the interval (in seconds) after which interim-accounting updates are sent
server [<1-6> [dscp <0-63>|host <WORD> secret <WORD> {port}|nai-routing| onboard|proxy-mode|retry-timeout-factor <50-200>|timeout]|preference]	Configures a RADIUS accounting server • <1-6> [dscp <0-63>|host <WORD> |nai-routing |onboard|proxy-mode|retry-timeout-factor <50-200>|timeout <1-60>] – Selects a server value to configure • dscp <0-63> – Specifies a Differentiated Services Code point values (QoS) used in generated RADIUS packets • <0-63> – Enter a DSCP value between 0 and 63 • host <WORD> – Displays the address of the server to be configured • <WORD> secret – Enter the IP address or hostname of the server • secret [0 <WORD>|2 <WORD>|<WORD>] {port} <1-65535> – Configures the RADIUS server shared secret • 0 <WORD> – Enter a clear text secret • 2 <WORD> – Enter an encrypted text secret • <WORD> {port} – Enter the shared secret, up to 127 characters • {port} <1-65535> – Configures the authentication port • <1-65535> – Configures the UDP port for accounting. The default port is 1812. • nai-routing realm-type – Configures Network Access Identifier based forwarding of requests • realm-type [prefix|suffix] – Select the match type made on the username • prefix realm <WORD> {strip} – Matches the prefix of the username (Eg: username is of type DOMAIN/user1, DOMAIN/user2) • suffix realm <WORD> {strip} – Matches the suffix of the username The following parameters are common for both prefix and suffix: • realm <WORD> – Enter the text matched against the username • <WORD> {strip} – Enter the matching text including the delimiter (delimiter is typically '' or '@') • {strip} – Strips the realm from the username before forwarding the request to the RADIUS server

	• onboard [controller|self] – Selects an onboard server instead of an external host
	  • controller – Configures the controller's RADIUS server to which the device is presently adopted
	  • self – Indicates the device itself
	• proxy-mode [none|through-controller|through-rf-domain-manager] – Select the mode of proxying requests from the list given below
	  • none – No proxy required. Send the request directly using the IP address of the device
	  • through-controller – Proxy the requests through the controller that is configuring the device
	  • through-rf-domain-manager – Proxy the requests through the local rf-domain-manager
	• retry-timeout-factor <50-200> – Configures the scaling of the retry timeout for this server between 50 and 200 seconds
	• timeout <1-60> {attempts} <1-10> – Configures the timeout in seconds for each request sent to the RADIUS server
	  • attempts <1-10> – Displays the number of times a transmission request is attempted
	  • <1-10> – Enter the number of attempts between 1 and 10
	• preference [auth-server-host|auth-server-number|none] – Configures the process in which a server from the pool is selected for sending authentication requests.
	  • auth-server-host – Prefers the same server host that was used for authentication
	  • auth-server-number – Prefers the same index/number of the server that was used for authentication
	  • none – Selects accounting server independent of which server was used for authentication

type [start-interim-stop|start-stop|stop-only]	Configures the type of RADIUS accounting packets sent • start-interim-stop – Sends Start message when the session begins, periodic Interim-Accounting updates, and finally an Accounting-Stop when the session ends • start-stop – Sends an Accounting-Start message when the session begins, and Accounting-Stop when the session ends • stop-only – Sends Accounting-Stop message when the session ends

Example

```
rfs7000-37FABE(config-aaa-policy-test)#accounting interim interval 65
rfs7000-37FABE(config-aaa-policy-test)#accounting server 2 host 172.16.10.10 secret
motorola port 1
rfs7000-37FABE(config-aaa-policy-test)#accounting server 2 nai-routing realm-type
prefix realm word strip
rfs7000-37FABE(config-aaa-policy-test)#accounting server 2 host word secret word port
6000
rfs7000-37FABE(config-aaa-policy-test)#accounting server 2 timeout 2 attempts 2
rfs7000-37FABE(config-aaa-policy-test)#accounting type start-stop
rfs7000-37FABE(config-aaa-policy-test)#accounting server preference auth-server-
number
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 accounting server 1 host 172.16.10.100 secret 0 testing
 accounting server 2 host 172.16.10.10 secret 0 motorola port 1008
```

```
accounting server 2 nai-routing realm-type prefix realm DSOS strip
accounting type start-interim-stop
accounting interim interval 65
accounting server preference auth-server-number
```

8.1.2 authentication

aaa-policy

Configures authentication parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
authentication [eap|protocol|server]
authentication eap wireless-client [attempts <1-10>|identity-request-timeout <1-
60>|retry-timeout-factor <50-200>|timeout <1-60>]
authentication protocol [chap|pap]
authentication server <1-6> [dscp|host|nac|nai-routing|onboard|
proxy-mode|retry-timeout-factor <50-200>|timeout]
authentication server <1-6> host <WORD> secret [0 <WORD> | 2 <WORD>|<WORD>] {port} <1-
65535>
authentication server <1-6> nac
authentication server <1-6> nai-routing realm-type [prefix|suffix] realm <WORD>
{strip}
authentication server <1-6> onboard [controller|self]
authentication server <1-6> proxy-mode [none|through-controller|through-rf-domain-
manager]
authentication server <1-6> timeout <1-60> {attempts} <1-10>
```

Parameters

eap wireless-client [attempts <1-10>|identity-request-timeout <1-60>|retry-timeout-factor <50-200>|timeout <1-60>]	Configures EAP parameters for clients • wireless-client – Configures EAP wireless client related parameters • attempts <1-10> – Enter the number of times a request is sent to a client • <1-10> – Specify the number of attempts • identity-request-timeout <1-60> – Enter the timeout value after which an EAP-Identity request message to a client is retried • <1-60> – Specify timeout in seconds • retry-timeout-factor <50-200> – Configures the mode the successive EAP retries are arranged • <50-200> – Enter the scaling factor between 50 and 200 seconds • timeout <1-60> – Specifies the timeout after which a request to a client is retried • <1-60> – Enter a timeout value between 1 and 60 seconds
protocol [chap|pap]	Configures the protocol used for non-EAP authentication • chap – Uses Challenge Handshake Authentication Protocol (CHAP) • pap – Uses Password Authentication Protocol (PAP)

server <1-6> [dscp|host|nac|nai-routing|onboard|proxy-mode|retry-timeout-factor <50-200>|time-out]	Configures an authentication server • <1-6> [dscp|host|nac|nai-routing|onboard|proxy-mode|retry-timeout-factor <50-200>|time-out] – Selects a server to be configured • dscp <0-63> – Specifies a differentiated devices code point value (QoS) to be used in generated RADIUS packets • <0-63> – Configures a DSCP value between 0 and 3 • host <WORD> – Defines the address of the server • <WORD> secret – Enter the IP address or hostname of the server • secret [0 <WORD>|2 <WORD>|<WORD>] *{port}* <1-65535> – Configures the RADIUS server shared secret • 0 <WORD> – Enter a clear text secret • 2 <WORD> – Enter an encrypted text secret • <WORD> {port} – Enter the shared secret • {port} <1-65535> – Configures the authentication port • <1-65535> – Enter the UDP port used for authentication. The default port is 1812. • nac – Uses the server for devices requiring network access control • nai-routing realm-type – Configures network access identifier based forwarding of requests • realm-type [prefix|suffix] – Select the match type made on the username • prefix realm <WORD> {strip} – Matches the prefix of the username • suffix realm <WORD> {strip} – Matches the suffix of the username The following parameters are common for both prefix and suffix: • realm <WORD> – Enter the text to be matched against the username • <WORD> {strip} – Enter the match text including the delimiter if applicable • {strip} – Strips the realm from the username before forwarding the request to the RADIUS server

	• onboard [controller|self] – Selects an onboard server instead of an external host
	  • controller – Specifies the onboard server on the controller to which the AP is adopted
	  • self – Specifies the onboard server on the device (AP or controller) where the client is associated
	• proxy-mode [none|through-controller|through-rf-domain-manager] – Selects the mode of proxying requests
	  • none – Sends the requests directly using the IP address of the device without proxy
	  • through-controller – Proxies the requests through the controller that is configuring the device
	  • through-rf-domain-manager – Proxies the requests through the local rf-domain-manager
	• retry-timeout-factor <50-200> – Configures the scaling of the retry timeout for the server. Enter a timeout value between 50 and 200 seconds
	• timeout <1-60> – Enter the timeout for each request sent to the RADIUS server
	  • <1-60> *{attempts}* – Enter the timeout in seconds
	  • attempts <1-10> – Enter the number of times a request is sent to the RADIUS server
	  • <1-10> – Enter the number of attempts required before a timeout

Example

```
rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 host 172.16.10.10
secret motorola port 1009
rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 timeout 10 attempts 3
rfs7000-37FABE(config-aaa-policy-test)#authentication server 5 nai-routing realm
-type suffix realm @motorola.com strip
rfs7000-37FABE(config-aaa-policy-test)#authentication protocol chap
rfs7000-37FABE(config-aaa-policy-test)#authentication eap wireless-client attempts 3
rfs7000-37FABE(config-aaa-policy-test)#authentication eap wireless-client identity-
request-timeout 20
rfs7000-37FABE(config-aaa-policy-test)#authentication server 2 onboard controller
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 onboard controller
 authentication server 5 timeout 20
 authentication server 5 nai-routing realm-type suffix realm @motorola.com strip
 accounting server 1 host 172.16.10.100 secret 0 testing
 accounting server 2 host 172.16.10.10 secret 0 motorola port 1008
 accounting server 2 nai-routing realm-type prefix realm DSOS strip
 authentication eap wireless-client identity-request-timeout 20
 authentication protocol chap
 accounting type start-interim-stop
 accounting interim interval 65
 accounting server preference auth-server-number
 authentication server 5 host 172.16.10.10 secret 0 motorola port 1009
 authentication server 5 timeout 20
 authentication server 5 host 172
```

8.1.3 mac-address-format

aaa-policy

Configures the format in which a MAC address must be filled in the RADIUS-request frames

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
    case [lower|upper] attributes [all|username-password]
```

Parameters]

mac-address-format [middle-hyphen|no-delim| pair-colon|pair-hyphen| quad-dot] case [lower|upper] attributes [all| username-password]	• middle-hyphen – Formatted as AABBCC-DDEEFF • no-delim – Formatted as AABBCCDDEEFF • pair-colon – Formatted as AA:BB:CC:DD:EE:FF • pair-hyphen – Formatted as AA-BB-CC-DD-EE-FF (default) • quad-dot – Formatted as AABB.CCDD.EEF The following parameters are common for all the above: • case [lower|upper] – Specifies whether the MAC address is to be filled in upper or lower case • lower – Uses lower case (Eg: aa-bb-cc-dd-ee-ff) • upper – Uses upper case (Eg: AA-BB-CC-DD-EE-FF) • attributes[all|username-password] – Specifies which RADIUS attributes will use the customized MAC address format • all – All attributes with MAC addresses (Username, Password, Calling-Station-Id, Called-Station-Id) • username-password – Specifies the username and password fields (which have the MAC address when mac-auth is used)

Example

```
rfs7000-37FABE(config-aaa-policy-test)#mac-address-format quad-dot case upper at
tributes username-password
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 mac-address-format quad-dot case upper attributes username-password
```

8.1.4 no

aaa-policy

Negates a command or sets its default values

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [accounting|authentication|mac-address-format|server-pooling-mode|use]
```

Parameters

accounting	Configures accounting parameters
authentication	Configures authentication parameters
mac-address-format	Resets the MAC address format used in requests to the default format
server-pooling-mode	Resets the method of selecting a server from the pool of configured AAA servers to its default values
use	Defines the settings used with this command

Usage Guidelines

Removes an access list control entry. Provide the rule-precedence value when using the no command.

Example

```
rfs7000-37FABE(config-aaa-policy-test)#no accounting dscp

rfs7000-37FABE(config-aaa-policy-test)#no mac-address-format

rfs7000-37FABE(config-aaa-policy-test)#no server-pooling-mode fail-through
rfs7000-37FABE(config-aaa-policy-test)#no authentication server 3 proxy-mode
rfs7000-37FABE(config-aaa-policy-test)#
```

8.1.5 server-pooling-mode

aaa-policy

Configures the method of selecting a server from the pool of configured AAA servers

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
server-pooling-mode [failover|load-balance]
```

Parameters

failover	Performs a failover starting from the first configured server
load-balance	Sends load-balance requests across all servers in the pool

Example

```
rfs7000-37FABE(config-aaa-policy-test)#server-pooling-mode load-balance
rfs7000-37FABE(config-aaa-policy-test)#server-pooling-mode load-balance
rfs7000-37FABE(config-aaa-policy-test)#sho context
aaa-policy test
 server-pooling-mode load-balance
```

8.1.6 use

aaa-policy

Applies a NAC for use by this aaa policy.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
use nac-list <NAC-LIST>
```

Parameters

nac-list <NAC-LIST>	Configures the Network Access Control related parameters • <NAC-LIST> – Enter an existing NAC list for use by this aaa-policy

Example

```
rfs7000-37FABE(config-aaa-policy-test)#use nac-list test1
rfs7000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 server-pooling-mode load-balance
 use nac-list test1
```

8.1.7 write

aaa-policy

Writes the running configuration to memory or a terminal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
write [memory|terminal]
```

Parameters

memory	Writes to the NV memory
terminal	Writes to a terminal

Example

```
rfs7000-37FABE(config-aaa-policy-test)#write terminal
!
! Configuration of RFS7000 version 5.1.0.0-036D
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 assignable-power-range 8 9
!
wlan-qos-policy default
!
radio-qos-policy default
!
aaa-policy default
!
association-acl-policy default
!
wips-policy default
!
hotspot-policy default
!
firewall ratelimit-trust policy default
!
management-policy default
 telnet
 http server
 ssh
!
!
firewall dos-attack policy default
!
firewall policy default
!
radius-server-policy default
```

```
!
mint-security-policy the_policy
!
role-policy default
!
device-discover-policy default
!
```

8.1.8 clrscr

aaa-policy

Clears the screen's current display

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clrscr
```

Parameters

None

Example

```
clrscr
```

8.1.9 commit

aaa-policy

Commits all the changes made in the active session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`commit {write}{memory}`

Parameters

write	If a commit succeeds, the configuration is written to the memory
memory	Writes to memory

Example

```
rfs7000-37FABE(config-aaa-policy-test)#commit write memory
[OK]
rfs7000-37FABE(config-aaa-policy-test)#
```

8.1.10 do

aaa-policy

Runs the commands from the EXEC mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
do <parameter>
```

Parameters

<parameter>	Displays parameters for which information can be viewed using the do command

Example

```
rfs7000-37FABE(config-aaa-policy-test)#do ?

ap-upgrade      AP firmware upgrade
 archive         Manage archive files
 boot            Boot commands
 cd              Change current directory
 change-passwd   Change password
 clear           Clear
 clock           Configure software system clock
 cluster         Cluster commands
 commit          Commit all changes made in this session
 configure       Enter configuration mode
 connect         Open a console connection to a remote device
 copy            Copy from one file to another
 crypto          Encryption related commands
 debug           Debugging functions
 delete          Deletes specified file from the system.
 diff            Display differences between two files
 dir             List files on a filesystem
 disable         Turn off privileged mode command
 edit            Edit a text file
 enable          Turn on privileged mode command
 erase           Erase a filesystem
 format          Format file system
 halt            Halt the system
 help            Description of the interactive help system
 logging         Modify message logging facilities
 mint            MiNT protocol
 mkdir           Create a directory
 more            Display the contents of a file
 no              Negate a command or set its defaults
 page            Toggle paging
 ping            Send ICMP echo messages
 pwd             Display current directory
 reload          Halt and perform a warm reboot
 remote-debug    Troubleshoot remote system(s)
 rename          Rename a file
 revert          Revert changes
```

```
rmdir           Delete a directory
self            Config context of the device currently logged into
telnet          Open a telnet connection
terminal        Set terminal line parameters
time-it           Check how long a particular command took between request and
                completion of response
traceroute      Trace route to destination
upgrade         Upgrade software image
upgrade-abort   Abort an ongoing upgrade
watch           Repeat the specific CLI command at a periodic interval
write           Write running configuration to memory or terminal

clrscr          Clears the display screen
exit            Exit from the CLI
service         Service Commands
show            Show running system information
```

8.1.11 end

aaa-policy

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to `the previous mode.`

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
end
```

Parameters

None

Example

```
rfs7000-37FABE(config-aaa-policy-test)#end
rfs7000-37FABE#
```

8.1.12 exit

aaa-policy

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to the previous mode.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE(config-aaa-policy-test)#exit
rfs7000-37FABE(config)#
```

8.1.13 health-check

aaa-policy

Configures server health-check parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
health-check interval <60-86400>
```

Parameters

interval<60-86400>	Configure an interval (in seconds) after which a server that was marked down earlier is checked again to see if it is now reachable • <60-86400> – Interval in seconds

Example

```
rfs7000-37FABE(config-aaa-policy-test)#health-check interval 4000
rfs7000-37FABE(config-aaa-policy-test)#
```

8.1.14 help

aaa-policy

Displays the interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`help search <WORD> {detailed|only-show|skip-no|skip-show}`

Parameters

search <WORD>	Searches for CLI commands related to a specific term • <WORD> *{detailed|only-show|skip-show}* – A term to search CLI commands for (Eg: a feature or a configuration parameter) • detailed – Searches and displays help strings in addition to mode and commands • only-show – Displays only the "show" commands, not configuration commands • skip-no – Does not display commands starting with "no" • skip-show – Displays only configuration commands, not "show" commands

Example

```
rfs7000-37FABE(config-aaa-policy-test)#help
When using the CLI, help is provided at the command line when typing '?'.

If no help is available, the help content will be empty. Backup until entering a
'?'shows the help content.

There are two styles of help provided:
1. Full help. Available when entering a command argument (e.g. 'show ?'). This will
describe each possible argument.

2. Partial help. Available when an abbreviated argument is entered. This will display
which arguments match the input (e.g. 'show ve ?').

rfs7000-37FABE(config-aaa-policy-test)#
```

8.1.15 revert

aaa-policy

Reverts the changes made to their last saved configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131xx
- AP650
- AP6511
- AP6532

Syntax

```
revert
```

Parameters

None

Example

```
rfs7000-37FABE(config-aaa-policy-test)#revert
rfs7000-37FABE(config-aaa-policy-test)#
```

8.1.16 service

aaa-policy

Displays service commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
service show cli
```

Parameters

show	Displays running system configuration
cli	Displays the CLI tree of the current mode

Example

```
rfs7000-37FABE(config-aaa-policy-test)#service show cli
AAA Policy Mode mode:
+-help [help]
+-show
  +-commands [show commands]
  +-running-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config) (|include-factory)]
  +-session-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config) (|include-factory)]
  +-device
    +-DEVICE [show device DEVICE (|include-factory)]
      +-include-factory [show device DEVICE (|include-factory)]
  +-session-changes [show session-changes]
  +-internal
    +-context
      +-running-config
       +-WORD [show internal context (running-config|session-config) WORD (|include-
factory)]
          +-include-factory [show internal context (running-config|session-config)
WORD (|include-factory)]
      +-session-config
       +-WORD [show internal context (running-config|session-config) WORD (|include-
factory)]
          +-include-factory [show internal context (running-config|session-config)
WORD (|include-factory)]
  +-startup-config [show startup-config (|include-factory)]
    +-include-factory [show startup-config (|include--DOMAIN-NAME [show wireless
mobile-unit (|(on DEVICE-OR-DOMAIN-NAME))]
      +-mac
        +-AA-BB-CC-DD-EE-FF [show wireless mobile-unit mac AA-BB-CC-DD-EE-FF (|(on
DEVICE-OR-DOMAIN-NAME))]
          +-on
           +-DEVICE-OR-DOMAIN-NAME [show wireless mobile-unit mac AA-BB-CC-DD-EE-FF
(|(on DEVICE-OR-DOMAIN-NAME))]
      +-statistics [show wireless mobile-unit statistics (|traffic) (|(on DEVICE-OR-
DOMAIN-
```

```
NAME))]..............................................................................
.........................
rfs7000-37FABE(config-aaa-policy-test)#
```

8.1.17 show

aaa-policy

Displays running system information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show <parameter>
```

Parameters

None

Example

```
adoption                Display information related to adoption to wireless
                        controller
advanced-wips           Advanced WIPS
ap-upgrade              AP Upgrade
boot                    Display boot configuration.
captive-portal          Captive portal commands
cdp                     Cisco Discovery Protocol
clock                   Display system clock
cluster                 Cluster Protocol
commands                Show command lists
context                 Information about current context
critical-resources      Critical Resources
crypto                  Encryption related commands
debug                   Debugging functions
debugging               Debugging functions
device-categorization   Device Categorization
event-history           Display event history
event-system-policy     Display event system policy
file                    Display filesystem information
firewall                Wireless Firewall
interface               Interface Configuration/Statistics commands
ip                      Internet Protocol (IP)
ip-access-list-stats    IP Access list stats
licenses                Show installed licenses and usage
lldp                    Link Layer Discovery Protocol
mac-access-list-stats   MAC Access list stats
mac-address-table       Display MAC address table
mint                    MiNT protocol
noc                     Noc-level information
ntp                     Network time protocol
password-encryption     Pasword encryption
power                   Show power over ethernet command
remote-debug            Show details of remote debug sessions
rf-domain-manager       Show RF Domain Manager selection details
role                    Role based firewall
running-config          Current operating configuration
session-changes         Configuration changes made in this session
session-config          This session configuration
sessions                Display CLI sessions
smart-rf                Smart-RF Management Commands
spanning-tree           Display spanning tree information
```

```
startup-config          Startup configuration
terminal                Display terminal configuration parameters
timezone                The timezone
upgrade-status          Display last image upgrade status
version                 Display software & hardware version
wireless                Wireless commands
```

CHAPTER 9 AUTO-PROVISIONING-POLICY

This chapter summarizes the auto-provisioning-policy commands in the CLI structure.

Adoption rules are sorted by precedence value and matched (filtered) against the information available from an AP, any rule for the wrong AP type is ignored.

For example,

```
rule #1 adopt ap7131 10 profile default vlan 10
rule #2 adopt ap650  20 profile default vlan 20
rule #3 adopt ap7131 30 profile default serial-number
rule #4 adopt ap7131 40 p d mac aa bb
```

AP7131 L2 adoption, VLAN 10 - will use rule #1

AP7131 L2 adoption, VLAN 20 - will not use rule #2 (wrong type), may use rule #3 if the serial number matched, else rule #4

If aa<= MAC <= bb, or else default.

Use the (config) instance to configure auto-provisioning-policy related configuration commands. To navigate to the auto-provisioning-policy instance, use the following commands:

```
rfs7000-37FABE(config)#auto-provisioning-policy  <policy-name>
rfs7000-37FABE(config)#auto-provisioning-policy test1
rfs7000-37FABE(config-auto-provisioning-policy-test1)#
Adoption Policy Mode commands:
  adopt              Add rule for device adoption
  default-adoption   Adopt devices even when no matching rules are found
                     Assign default profile and default rf-domain
  deny               Add rule to deny device adoption
  no                 Negate a command or set its defaults

  clrscr             Clears the display screen
  commit             Commit all changes made in this session
  do                 Run commands from Exec mode
  end                End current mode and change to EXEC mode
  exit               End current mode and down to previous mode
  help               Description of the interactive help system
  revert             Revert changes
  service            Service Commands
  show               Show running system information
  write              Write running configuration to memory or terminal

rfs7000-37FABE(config-auto-provisioning-policy-test)#
```

9.1 auto-provisioning-policy

Table 9.1 Summarizes auto-provisioning-policy commands

Table 9.1 *auto-provisioning-policy commands*

Command	Description	Reference
adopt	Adds rules for device adoption	*page 9-3*
default-adoption	Adopts devices even when no matching rules are found. Assigns default profile and default rf-domain	*page 9-6*
deny	Adds a rule to deny device adoption	*page 9-7*
no	Negates a command or sets its default value	*page 9-9*

9.1.1 adopt

auto-provisioning-policy

Adds rules for device adoption

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
adopt [ap7131|ap650|ap6511|ap6532|]

adopt [ap7131|ap650|ap6511||ap6532] <1-1000> <PROFILE>
<RF-DOMAIN> [any|cdp-match <WORD>|dhcp-option <WORD>|fqdn <WORD>|ip|lldp-match
<WORD>|mac|model-number <WORD>|serial-number <WORD>|vlan <VLAN-ID>]

adopt [ap7131|ap650|ap6511|ap6532] <1-1000> <PROFILE>
<RF-DOMAIN> ip [<Starting IP> <Ending IP>|<A.B.C.D/M>]

adopt [ap7131|ap650|ap6511|6532] <1-1000> <PROFILE>
<RF-DOMAIN> mac <Starting MAC> {<Ending MAC>}
```

Parameters

adopt [ap7131|ap650|ap6511|ap6532] <1-1000> <PROFILE> <RF-DOMAIN> [any|cdp-match <WORD>|dhcp-option <WORD>|fqdn <WORD>|ip|lldp-match <WORD>|mac|model-number <WORD>|serial-number <WORD>|vlan <VLAN-ID>]	Adds rules for device adoption • ap7131– Configures an AP7131 • ap650 – Configures an AP650 • ap6511 – Configures an AP6511 • ap6532 – Configures an AP6532 The following parameters are common for all the APs: • <1-1000> – Configure a rule precedence value between 1 and 1000 • <PROFILE> – Enter the name of the profile to use • <RF-DOMAIN> – Enter the RF-Domain device to use • ny – Matches any device • cdp-match <WORD> – Matches device location based on CDP snoop • <WORD> – Specify the location substring to match • dhcp-option <WORD> – Matches the value of DHCP option • <WORD> – Enter the DHCP option name • fqdn <WORD> – Matches the value of FQDN • <WORD> – Specify the value to match • ip [<Starting IP> <Ending IP>|<A.B.C.D/M>] – Matches device IP address • <Starting IP> <Ending IP> – Enter a beginning and an ending IP address range to configure • <A.B.C.D/M> – Enter the IP address to configure • lldp-match <WORD> – Matches device location based on LLDP snoop • <WORD> –Specify the location substring to match • mac <Starting MAC> <Ending MAC> – Matches device MAC address • <Starting MAC> <Ending MAC> – Enter a starting and ending MAC address from a range of MAC addresses. An ending MAC address is optional. • model number <WORD> – Matches device model number • <WORD> – Enter the matching device model number • serial-number <WORD> – Matches device serial number • <WORD> – Enter the matching device serial number • vlan <VLAN-ID> – Matches device VLAN • <VLAN-ID> – Enter a target VLAN ID

Example

```
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt ap7131 10 ap7131 default
vlan 1
rfs7000-37FABE(config-auto-provisioning-policy-test)#commit write memory
rfs7000-37FABE(config-auto-provisioning-policy-test)#show wireless ap
+---+--------------+---------+-------------+--------------+
|IDX|NAME  |MAC  |TYPE|SERIAL-NUMBER |ADOPTION-MODE|   VERSION    |
+---+--------------+---------+-------------+--------------+
| 1 | ap7131-889EC4 | 00-15-70-88-9E-C4 | AP7131 | 8164520900006 | L2: vlan1   |
5.0.0.0-055D |
+---+--------------+------------------+--------+--------------+--------


rfs7000-37FABE(config-auto-provisioning-policy-test)#show wireless ap configured
+-----+----------------+--------------------+-----------------+--------
```

```
| IDX |       NAME       |         MAC          |     PROFILE       |  RF-DOMAIN  |
+-----+------------------+----------------------+-------------------+--------
| 1   | ap7131-889EC4    | 00-15-70-88-9E-C4    | default-ap7131    | default     |
| 2   | ap650-445566     | 11-22-33-44-55-66    | default-ap650     | default     |
+-----+------------------+----------------------+-------------------+--------
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt ap7131 10 ap7131 default
dhcp-option test
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt ap7131 10 ap7131 default
ip 172.16.10.3 172.16.10.4
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt ap7131 10 ap7131 default
ip 172.16.10.3/24
rfs7000-37FABE(config-auto-provisioning-policy-test)#adopt ap7131 10 ap7131 default
mac 11-22-33-44-55-66
rfs7000-37FABE(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap7131 10 ap7131 default vlan 1
rfs7000-37FABE(config-auto-provisioning-policy-test)#
```

9.1.2 default-adoption

auto-provisioning-policy

Adopts devices even when no matching rules are found. Assigns a default profile and default RF Domain

Supported in the following platforms:

- RFS7000
- RFS6000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
default-adoption
```

Parameters

None

Example

```
rfs7000-37FABE(config-auto-provisioning-policy-test)#default-adoption
rfs7000-37FABE(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
```

9.1.3 deny

auto-provisioning-policy

Adds a rule to deny device adoption

Supported in the following platforms:

- RFS7000
- RFS6000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
deny [ap7131|ap650|ap6511|ap6532] <1-1000>  [any|cdp-match <WORD>|dhcp-option
<WORD>|fqdn <WORD>|ip|lldp-match <WORD>|mac|model-number <WORD>|serial-number
<WORD>|vlan <VLAN-ID>]

deny [ap7131|ap650|ap6511|ap6532] <1-1000>  ip [<Starting IP> <Ending IP>|A.B.C.D/M]

deny [ap7131|ap650|ap6511|ap6532] <1-1000>  mac <Starting MAC> {<Ending MAC>}
```

Parameters

[ap7131|ap650|ap6511| ap6532] <1-1000> [any|cdp-match <WORD>|dhcp-option <WORD>|fqdn|ip|lldp-match <WORD>|mac|model-number <WORD>|serial-number <WORD>|vlan <VLAN-ID>]	Use the 'deny' command to add a rule to deny a device adoption • ap7131 – Configures an AP7131 • ap650 – Configures an AP650 • ap6511 – Configures an AP6511 • ap6532 – Configures an AP6532 The following parameters are common for both AP7131 and AP650: • <1-1000> – Configure a rule precedence value between 1 and 1000 • any – Matches any device • cdp-match <WORD> – Matches device location based on CDP snoop • <WORD> – Specify the location substring to match • dhcp option <WORD> – Matches the value of DHCP option • <WORD> – Enter the DHCP option name • fqdn <WORD> – Matches the value of FQDN • <WORD> – Specify the value to match • ip [<Starting IP> <Ending IP>|<A.B.C.D/M>] – Matches device IP address • <Starting IP> <Ending IP> – Enter a beginning and an ending IP address range to configure • <A.B.C.D/M> – Enter the IP address to configure • lldp-match <WORD> – Matches device location based on LLDP snoop • <WORD> – Specify the location substring to match • mac <Starting MAC > *{<Ending MAC>}* – Matches device MAC address • <Starting MAC> <Ending MAC> – Enter a starting and ending MAC address of a range on MAC addresses. Ending MAC address is optional. • model number <WORD> – Matches device model number • <WORD> – Enter the matching device model number • serial number <WORD> – Matches device serial number • <WORD> – Enter the matching device serial number • vlan <VLAN-ID> – Matches device VLAN • <VLAN-ID> – Enter a target VLAN ID

Example

```
rfs7000-37FABE(config-auto-provisioning-policy-test)#deny ap7131 600 vlan 1
rfs7000-37FABE(config-auto-provisioning-policy-test)#deny ap7131 600 ip 172.16.10.1/
24
rfs7000-37FABE(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 deny ap71xx 100 vlan 20
 deny ap71xx 101 ip 172.16.11.0/24
```

9.1.4 no

auto-provisioning-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [adopt|default-adoption|deny]
```

Parameters

[adopt| default-adoption|deny]	• adopt – Removes an adoption rule • default-adoption – Does not adopt a device if no matching rules apply • deny – Removes a deny rule

Example

```
rfs7000-37FABE(config-auto-provisioning-policy-test1)#no default-adoption
rfs7000-37FABE(config-auto-provisioning-policy-test1)#
```

NOTE: The commands clrscr, commit, exit, help, write, revert, service and show are common commands. Refer to *Chapter 5, COMMON COMMANDS* for more information.

CHAPTER 10 ADVANCED-WIPS-POLICY

This chapter summarizes the advanced-wips-policy commands within the CLI structure.

Use the (config) instance to configure advance-wips-policy related configuration commands. To navigate to the advanced-wips-policy instance, use the following commands:

```
rfs7000-37FABE(config)#advanced-wips-policy <policy-name>
rfs7000-37FABE(config)#advanced-wips-policy test
rfs7000-37FABE(config-advanced-wips-policy-test)#
rfs7000-37FABE(config-advanced-wips-policy-test)#?
Advanced WIPS policy Mode commands:
  event                Configure event detection
  no                   Negate a command or set its defaults
  server-listen-port   Configure local WIPS server listen port number
  terminate            Add a device to the list of devices to be terminated
  use                  Set setting to use

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal
rfs7000-37FABE(config-advanced-wips-policy-test)#
```

10.1 advanced-wips-policy

Table 10.1 Summarizes advanced-wips-policy commands

Table 10.1 *advanced-wips-policy commands*

Command	Description	Reference
event	Configures events	*page 10-3*
no	Negates a command or sets its default value	*page 10-8*
server-listen-port	Sets a local WIPS server's listening port	*page 10-9*
terminate	Adds a device to a list of devices terminated	*page 10-10*
use	Defines the settings used with the advanced-wips-policy	*page 10-11*

10.1.1 event

advanced-wips-policy

Configures event detection. Configures the parameters related to the detection of anomalous frames on the RF network.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
event [accidental-association|all|crackable-wep-iv-used|dos-cts-flood|
   dos-deauthentication-detection|dos-disassociation-detection|
   dos-eap-failure-spoof|dos-eapol-logoff-storm|dos-rts-flood|
   essid-jack-attack-detected| fake-dhcp-server-detected|fata-jack-detected|
   id-theft-eapol-success-spoof-detected|id-theft-out-of-sequence|
   invalid-channel-advertized|invalid-management-frame|ipx-detection|
   monkey-jack-attack-detected|multicast-all-routers-on-subnet|
   multicast-all-systems-on-subnet| multicast-dhcp-server-relay-agent|
   multicast-hsrp-agent|multicast-igmp-detection|multicast-igmp-routers-detection|
   multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detection|
   multicast-rip2-routers-detection|multicast-vrrp-agent|netbios-detection|
   null-probe-response-detected|probe-response-flood|rogue-ap-detection|
   stp-detection|unauthorized-bridge|windows-zero-config-memory-leak|
   wlan-jack-attack-detected]

event [accidental-association|rogue-ap-detection|unauthorized-bridge]
   [mitigation-enable|trigger-against {neighboring|sanctioned|unsanctioned}]

event all trigger-all-applicable
event crackable-wep-iv-used trigger-against {neighboring|sanctioned|unsanctioned}
event dos-cts-flood [threshold [cts-frames-ratio |
mu-rx-cts-frames]<0-65535> |trigger-against
{neighboring|sanctioned|unsanctioned}]

event [dos-deauthentication-detection|dos-disassociation-detection|
   dos-eap-failure-spoof|dos-rts-flood|essid-jack-attack-detected|
   fake-dhcp-server-detected|fata-jack-detected|
   id-theft-eapol-success-spoof-detected|id-theft-out-of-sequence|
   invalid-channel-advertized|invalid-management-frame|ipx-detection|
   monkey-jack-attack-detected|multicast-all-routers-on-subnet|
   multicast-all-systems-on-subnet|multicast-dhcp-server-relay-agent|
   multicast-hsrp-agent|multicast-igmp-detection|multicast-igmp-routers-detection|
   multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detection|
   multicast-rip2-routers-detection|multicast-vrrp-agent|netbios-detection|
   null-probe-response-detected|stp-detection|windows-zero-config-memory-leak|
   wlan-jack-attack-detected] trigger-against{neighboring|sanctioned|unsanctioned}]

event dos-eapol-logoff-storm [threshold [eapol-start-frames-ap|eapol-start-frames-
mu]<0-65535> |trigger-against {neighboring|sanctioned|unsanctioned}]
event probe-response-flood [threshold  probe-rsp-frames-count
<0-65535>|trigger-against {neighboring|sanctioned|unsanctioned}]]
```

Parameters

event [accidental-association|rogue-ap-detection|unauthorized-bridge] [mitigation-enable|trigger-against *{neighboring|sanctioned|unsanctioned}*]	Configures parameters related to the detection of anomalous frames on the RF network. The parameters are:
	• accidental-association – Detects an accidental client association
	• rogue-ap-detection – Detects a rogue AP
	• unauthorized-bridge – Detects an unauthorized bridge
	The following parameters are common for the above:
	• mitigation-enable – Enables the mitigation for the event
	• trigger-against *{neighboring|sanctioned|unsanctioned}* – Sets a trigger from the list
	  • neighboring – Triggers against neighboring (ignored) devices
	  • sanctioned – Triggers against sanctioned (approved) devices
	  • unsanctioned – Triggers against unsanctioned (unapproved) devices

all trigger-all-applicable	Detects all the events

dos-cts-flood [threshold [cts-frames-ratio | mu-rx-cts-frames]<0-65535> |trigger-against *{neighboring|sanctioned|unsanctioned}*	Detects DoS CTS Flood
	• threshold [cts-frames-ratio |mu-rx-cts-frames] – Configures the event's threshold
	  • cts-frames-ratio <0-65535> – CTS/Total Frames ratio in a percentage
	  • mu-rx-cts-frames <0-65535> – Threshold for CTS frames received by a client
	  • <0-65535> – Specify a threshold value between 0 and 65535
	• trigger-against *{neighboring|sanctioned|unsanctioned}* – Sets the trigger from the list
	  • neighboring – Triggers against neighboring (ignored) devices
	  • sanctioned – Triggers against sanctioned (approved) devices
	  • unsanctioned – Triggers against unsanctioned (unapproved) devices

[crackable-wep-iv-used|dos-deauthentication-detection|dos-disassociation-detection|dos-eap-failure-spoof|dos-rts-flood|essid-jack-attack-detected|fake-dhcp-server-detected|fata-jack-detected|id-theft-eapol-success-spoof-detected|id-theft-out-of-sequence|invalid-channel-advertized|invalid-management-frame|ipx-detection|monkey-jack-attack-detected|multicast-all-routers-on-subnet|multicast-all-systems-on-subnet|multicast-dhcp-server-relay-agent|multicast-hsrp-agent|multicast-igmp-detection|multicast-igmp-routers-detection|multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detection|multicast-rip2-routers-detection	• crackable-wep-iv-used – Detects crackable WEP IV used • dos-deauthentication-detection – Detects DoS deauthentication • dos-disassociation-detection – Detects DoS disassociation • dos-eap-failure-spoof – Detects a DoS EAP failure spoof • dos-rts-flood – Detects a DoS RTS flood • essid-jack-attack-detected – Detects an ESSID jack attack • fake-dhcp-server-detected – Detects a fake DHCP server • fata-jack-detected – Detects a fata-jack attack • id-theft-eapol-success-spoof-detected – Detects an ID theft - EAPOL success spoof • id-theft-out-of-sequence – Detects an ID theft - out of sequence • invalid-channel-advertized – Detects an invalid channel advertizement • invalid-management-frame – Detects an invalid management frame • ipx-detection – Detects IPX • monkey-jack-attack-detected – Detects a monkey-jack attack • multicast-all-routers-on-subnet – Detects all multicast routers in the subnet • multicast-all-systems-on-subnet – Detects all multicast systems on the subnet • multicast-dhcp-server-relay-agent – Detects multicast DHCP server relay agents • multicast-hsrp-agent – Detects multicast HSRP agents • multicast-igmp-detection – Detects multicast IGMP • multicast-igrp-routers-detection – Detects multicast IGRP routers • multicast-ospf-all-routers-detection – Detects multicast OSPF all routers
multicast-vrrp-agent|netbios-detection|null-probe-response-detected|stp-detection|windows-zero-config-multicast-rip2-routers-detection|memory-leak|wlan-jack-attack-detected] trigger-against *{neighboring|sanctioned|unsanctioned}*	• multicast-ospf-designated-routers-detection – Detects multicast OSPF designated routers • multicast-rip2-routers-detection – Detects multicast RIP2 routers • multicast-vrrp-agent – Detects multicast VRRP agents • netbios-detection – Detects NetBIOS • null-probe-response-detected – Detects null probe response • stp-detection – Detects STP • windows-zero-config-memory-leak – Detects windows zero config memory leak • wlan-jack-attack-detected – Detects WLAN jack attacks The following parameters are common for all the above: • trigger-against *{neighboring|sanctioned|unsanctioned* – Sets the trigger from the list • neighboring – Triggers against Neighboring (Ignored) devices • sanctioned – Triggers against Sanctioned (sanctioned) devices • unsanctioned – Triggers against Unsanctioned (Unsanctioned) devices

dos-eapol-logoff-storm [threshold [eapol-start-frames-ap|eapol-start-frames-mu]<0-65535> |trigger-against *{neighboring|sanctioned|unsanctioned}*]	Detects DoS EAPoL Logoff Storm • threshold – Configures the event threshold • eapol-start-frames-ap <0-65535> –Detects EAPoL start frames transmitted by an AP • eapol-start-frames-mu <0-65535> – Detects EAPoL start frames transmitted by a client • <0-65535> – Select a threshold value between 0 and 65535 • trigger-against *{neighboring|sanctioned|unsanctioned}* – Sets the trigger from the list • neighboring – Triggers against neighboring ignored) devices • sanctioned – Triggers against sanctioned (approved) devices • unsanctioned – Triggers against unsanctioned (unapproved) devices
probe-response-flood [threshold probe-rsp-frames-count <0-65535>|trigger-against *{neighboring| sanctioned|unsanctioned}*]	Detects Probe Response Flood values • threshold probe-rsp-frames-count <0-65535> – Configures the event threshold • probe-rsp-frames-count <0-65535> – Count for probe response frames transmitted by an AP • <0-65535> – Select a threshold value between 0 and 65535 • trigger-against *{neighboring|sanctioned|unsanctioned}* – Sets the trigger from the list • neighboring – Triggers against neighboring (ignored) devices • sanctioned – Triggers against sanctioned (approved) devices • unsanctioned – Triggers against unsanctioned (unapproved) devices

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#event dos-cts-flood threshold cts-
frames-ratio 8
rfs7000-37FABE(config-advanced-wips-policy-test)#event dos-eapol-logoff-storm
threshold eapol-start-frames-mu 99
rfs7000-37FABE(config-advanced-wips-policy-test)#event probe-response-flood
threshold probe-rsp-frames-count 8
rfs7000-37FABE(config-advanced-wips-policy-test)#event wlan-jack-attack-detected
trigger-against sanctioned
rfs7000-37FABE(config-advanced-wips-policy-test)#event probe-response-flood trigger-
against sanctioned
```

10.1.2 no

advanced-wips-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [event|server-listen-port|terminate|use]
```

Parameters

event	Configures event detection
server-listen-port	Sets a local WIPS server's listening port
terminate	Removes a device from the device termination list
use	Defines settings to use with the advanced WIPS policy

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#no event accidental-association
trigger-against
rfs7000-37FABE(config-advanced-wips-policy-test)#no server-listen-port
```

10.1.3 server-listen-port

advanced-wips-policy

Configures the local WIPS server's listening port

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
server-listen-port <0-65535>
```

Parameters

server-listen-port <0-65535>	Select a port number between 0 and 65535 for the WIPS sensors to connect to the server

NOTE: Onboard WIPS uses port 8443 and AirDefense Enterprise uses 443

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#server-listen-port 1009
```

10.1.4 terminate

advanced-wips-policy

Adds a device to the termination list

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
terminate <AA-BB-CC-DD-EE-FF>
```

Parameters

terminate <AA-BB-CC-DD-EE-FF>	Specify a target termination device MAC address in a AA-BB-CC-DD-EE-FF format

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#terminate 00-40-96-B0-BA-2D
```

10.1.5 use

advanced-wips-policy

Sets the device categorizations settings for the specified device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
use device-categorization <WORD>
```

Parameters

device-categorization <WORD>	Creates/Configures device categorization list • <WORD> – Specify a device name to be associated to this profile

NOTE: advanced-wips ignores the SSID of marked devices for device-categorization

Example

```
rfs7000-37FABE(config-advanced-wips-policy-test)#use device-categorization rfs7000
Please note, advanced-wips ignores SSID of marked devices
;rfs7000-37FABE(config-advanced-wips-policy-test)#
```

NOTE: The commands clrscr, commit, exit, help, write, revert, service and show are common commands. For more information, see *Chapter 5, COMMON COMMANDS*.

CHAPTER 11 ASSOCIATION-ACL-POLICY

This chapter summarizes the association-acl-policy commands within the CLI structure.

Use the (config) instance to configure association-acl-policy related configuration commands. To navigate to the association-acl-policy instance, use the following commands:

```
rfs7000-37FABE(config)#association-acl-policy  <policy-name>
rfs7000-37FABE(config-assoc-acl-test)# association-acl-policy test
rfs7000-37FABE(config-assoc-acl-test)#
rfs7000-37FABE(config-assoc-acl-test)#?
Association ACL Mode commands:
  deny     Specify MAC addresses to be denied
  no       Negate a command or set its defaults
  permit   Specify MAC addresses to be permitted

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal
rfs7000-37FABE(config-assoc-acl-test)#
```

11.1 association-acl-policy

Table 11.1 Summarizes association-acl-policy commands

Table 11.1 *association-acl-policy*

Command	Description	Reference
deny	Specifies a range of denied MAC addresses	*page 11-3*
no	Negates a command or sets its default value	*page 11-4*
permit	Specifies a range of permitted MAC addresses	*page 11-5*

11.1.1 deny

association-acl-policy

Specifies a range of denied MAC addresses

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
deny  <Starting-MAC> [<Ending-MAC>|precedence <1-1000>]
deny <Staring-MAC> <Ending-MAC> precedence <1-1000>
```

Parameters

<Starting-MAC> [<Ending-MAC>|precedence <1-1000>]	Enter the starting MAC address in a range of denied MAC addresses • <Ending-MAC> precedence <1-1000> – Enter the ending MAC address of a range of MAC addresses. (Optional if a single MAC is added) • precedence <1-1000> – Enter a precedence value between 1 and 1000 (rules are checked in an increasing order of precedence)

Example

```
rfs7000-37FABE(config-assoc-acl-test)#deny 00-40-96-B0-BA-2D precedence 2
rfs7000-37FABE(config-assoc-acl-test)#
```

11.1.2 no

association-acl-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [deny|permit]
```

Parameters

[deny|permit]	• deny – Enter a deny rule to delete • permit – Enter a permit rule to delete

Example

```
rfs7000-37FABE(config-assoc-acl-test)#no deny 00-40-96-B0-BA-2D precedence 2
rfs7000-37FABE(config-assoc-acl-test)#
```

11.1.3 permit

association-acl-policy

Specifies a range of permitted MAC addresses

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
permit  <Starting-MAC> [<Ending-MAC>|precedence <1-1000>]
permit <Staring-MAC> <Ending-MAC> precedence <1-1000>
```

Parameters

<Starting-MAC> [<Ending-MAC>|precedence <1-1000>]	Enter the starting MAC address in a range of permitted MAC addresses • <Ending-MAC> precedence <1-1000> – Enter the ending MAC address in a range of MAC addresses. Optional, if a single MAC is added • precedence <1-1000> – Enter a precedence value between 1 and 1000 (rules are checked in an increasing order of precedence)

Example

```
rfs7000-37FABE(config-assoc-acl-test)#permit 00-40-96-B0-BA-2D precedence 3
rfs7000-37FABE(config-assoc-acl-test)#
```

NOTE: clrscr, commit, do, exit, help, write, revert, service and show are common commands. For more information, see *Chapter 5, COMMON COMMANDS*.

Chapter 12 ACCESS-LIST

This chapter summarizes IP and MAC access list commands in detail.

Access-lists control access to the network through a set of rules. Each rule specifies an action taken when a packet matches a given set of rules. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. The controller supports the following ACLs.

- IP access lists
- MAC access lists

Use IP and MAC commands under the global configuration to create an access list.

- When the access list is applied on an Ethernet port, it becomes a port ACL
- When the access list is applied on a VLAN interface, it becomes a router ACL

Use the (config) instance to configure access-list related configuration commands. To navigate to the (config-access-list) instance, use the following commands.

ip-access-list

```
rfs7000-37FABE(config)#ip access-list test
rfs7000-37FABE(config-ip-acl-acl)#?
ACL Config commands:
  deny      Specify packets to reject
  no        Negate a command or set its defaults
  permit    Specify packets to forward
  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal
rfs7000-37FABE(config-ip-acl-acl)#
```

mac-access-list

```
rfs7000-37FABE(config)#mac access-list test
rfs7000-37FABE(config-mac-acl-test)#?
MAC Extended ACL Config commands:
  deny      Specify packets to reject
  no        Negate a command or set its defaults
  permit    Specify packets to forward
  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal
rfs7000-37FABE(config-mac-acl-test)#
```

12.1 ip-access-list

Table 12.1 Summarizes commands under the IP access list mode

Table 12.1 *ip-access-list commands*

Command	Description	Reference
clrscr	Clears the display screen	*page 12-18*
commit	Commits the changes made in the current session	*page 12-19*
deny	Specifies packets to reject	*page 12-4*
end	Ends and exits the current mode and moves to the PRIV EXEC mode	*page 12-20*
exit	Ends the current mode and moves to the previous mode	*page 12-21*
help	Displays the interactive help system	*page 12-22*
no	Negates a command or sets its default value	*page 12-15*
permit	Permits specific packets	*page 12-9*
revert	Reverts changes made to their last saved configuration	*page 12-23*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 12-24*
show	Displays running system information	*page 12-26*
write	Writes information to memory or terminal	*page 12-16*

12.1.1 deny

ip-access-list

Specifies packets to reject

NOTE: Use a decimal value representation of ethertypes to implement a `permit/deny` designation for a packet. The command set for IP ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
deny [icmp|ip|proto|tcp|udp]

deny icmp [<source-IP>|any|host <IP>] [<dest-IP>|any|host <IP>] {<ICMP-type> {<ICMP-
code>}} {log} {rule-precedence <1-5000>}] <0-255>

deny ip [<source-IP>|any|host <IP>] [<dest-IP>|any|host <IP>] {log} {rule-precedence
<1-5000>}

deny [tcp|udp] [<source-IP>|any|host <IP>] {eq
<source-port>|range <starting-source-port>
<ending-source-port>} [<dest-IP|any|host <IP>]
{eq <source-port>} {range <starting-source-port>
<ending-source-port>} {eq[<1-65535>|<WORD>|bgp|dns|ftp|ftp
|gopher|https|ldap|nntp|ntp|pop3|smtp|ssh | telnet |tftp| www} {log} {rule-precedence
<1-5000>

deny proto [<0-254>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp][<source-IP/
Mask>|any|host <IP>][<dest-IP/Mask>|any|host <IP>] {log} {rule-description
<WORD>|rule-precedence<1-5000>}
```

Parameters

deny ip [<source-IP>|any|host <IP>][<dest-IP>|any|host <IP>] {log} {rule-precedence <1-5000>}	Use with the deny command to reject packets • deny – Sets the action type on an ACL • IP – Specifies an IP address • <source-ip>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format. • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <ip> (A.B.C.D format) and source-mask bits equal to 32 • <dest-IP>|any|host <IP> – Defines the destination host IP address or destination network address • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL
deny icmp [<source-IP>|any|host <IP>] [<dest-IP>|any|host <IP>] {<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>}	Use with the deny command to reject ICMP packets • deny – Rejects ICMP packets • icmp – Specifies ICMP as the protocol • <source-ip>|any|host <IP>] – The source <source-IP> is the source IP address of the network or host (in dotted decimal format) • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32 • <dest-IP>|any|host <IP>] – Defines the destination host IP address or destination network address • <ICMP-type> {<ICMP-code>} – Sets the ICMP type value <ICMP-type> from 0 to 255, and is valid only for ICMP. The ICMP code value <ICMP-code> is from 0 to 255, and is valid only for ICMP • log – Generates log messages when a packet coming from an interface matches an ACL entry. Log messages are generated only for router ACLs • rule-precedence <1-5000> – Optional. Defines an integer value between 1-5000. This value sets the rule precedence in the ACL

deny [tcp|udp] [<source-IP>|any|host <IP>] {eq <source-port>|range <starting-source-port> <ending-source-port>} [<dest-IP|any|host <IP>]{eq <source-port>} {range <starting-source-port> <ending-source-port>} {eq [<1-65535> | <WORD>|bgp|dns|ftp|ftp |gopher|https|ldap|nntp|ntp|pop3|smtp|ssh | telnet |tftp| www}{log} {rule-precedence <1-5000>}	Use with the deny command to reject TCP or UDP packets • deny – Rejects TCP or UDP packets • [tcp|udp] – Specifies TCP or UDP as the protocol • <source-IP>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535 • range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers) • <dest-IP>|any|host <IP> – Defines the destination host IP address or destination network address • eq <source-port> {range <starting-source-port> <ending-source-port>} – Defines a specific destination port • range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535 • <1-65535> – Destination port • <WORD> – Displays any Service Name • bgp – Bgp port 179 • dns – DNS port 53 • ftp – Ftp-ctrl port 21 • ftp-data – Ftp-data port 20 • gopher – Gopher port 70 • https – HTTPS port 443 • ldap – LDAP port 389 • nntp – NNTP port 119 • ntp – NTP port 123 • pop3 – Pop3 port 110 • smtp – SMTP port 25 • ssh – SSH port 22 • telnet – Telnet port 23 • tftp – TFTP port 69 • www – HTTP port 80 • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL

[<0-254>|<WORD>| eigrp|gre|igmp|igp|ospf|vrrp][<source-IP/Mask>|any|host <IP>][<dest-IP/Mask>|any|host <IP>] {log} {rule-description <WORD>|rule-precedence<1-5000>}]	Use with the deny command to deny any protocol other than TCP, UDP or ICMP • <0-254] – Displays the protocol number • <WORD> – Refers to any protocol name • eigrp – EIGRP protocol 88 • gre – GRE protocol 47 • igmp – IGMP protocol 2 • igp – IGP protocol 9 • ospf – OSPF protocol 89 • vrrp – VRRP protocol 112 • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • <dest-IP/mask>|any|host <IP> – Defines the destination host IP address or destination network address • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • rule-description <WORD> – Defines access-list entry name

Usage Guidelines

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- ip
- icmp
- tcp
- udp
- proto

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

- Filtering TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP as the protocol to allow/deny ICMP packets. Selecting ICMP provides the option of filtering ICMP

packets based on ICMP type and code

NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

Example

```
rfs7000-37FABE(config-ip-acl-test)#deny icmp 172.16.10.3/24 any rule-precedence 88
rfs7000-37FABE(config-ip-acl-test)#
rfs7000-37FABE(config-ip-acl-test)#deny icmp 172.16.10.3/24 host 172.16.10.7 8 log
rule-precedence 99
rfs7000-37FABE(config-ip-acl-test)#
```

12.1.2 permit

ip-access-list

Permits specific packets

NOTE: Use a decimal value representation of ethertypes to implement a `permit/deny` designation for a packet. The command set for IP ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
permit[icmp|ip|tcp|upd|proto]
permit proto [<0-255>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp][<source-IP/
Mask>|any|host <IP>][<dest-IP/Mask>|any|host <IP>] {log} {rule-description
<WORD>|rule-precedence<1-5000>} {mark [8021p <0-7>|
dscp <0-63>]{rule-description <WORD>|rule-precedence<1-5000>}}]
```

```
permit [tcp|udp] [<source-IP/Mask>|host <IP>|any] [<dest-IP/Mask>|host <IP>|any] {eq
<1-65535> | range <1-65535> <1-65535>} {eq [<1-65535> | <WORD>|bgp|dns|ftp|ftp
|gopher|https|ldap|nntp|ntp|pop3|smtp|ssh | telnet |tftp| www}|range <1-
65535>|log|mark [8021p <0-7>|dscp <0-63>] rule-precedence <1-5000> {rule-description}
<WORD> |rule-precedence <1-5000> {rule-description} <WORD>}
```

```
permit [icmp|ip] [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host <IP>]
{any[<0-255> <0-255>} {log} {mark [8021p <0-7>|dscp<0-63>  rule-precedence <1-5000>
{rule-description} <WORD> } {rule-precedence <1-5000> {rule-description} <WORD>}
```

Parameters

permit ip [<source-IP/Mask>| any|host <IP>] [<dest-IP/Mask>|any|host <IP>] {log} {rule-precedence <1-5000>} {mark [8021p <0-7>|dscp<0-63> rule-precedence <1-5000> {rule-description} <WORD>}	Use with a permit command to allow IP packets • permit – Sets the action type on an ACL • IP – Specifies an IP (to match to a protocol) • <source-IP/Mask>|any|host <IP> – The keyword <source-IP> is the source IP address of the network or host in dotted decimal format • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for the exact source <IP> (A.B.C.D format) and source-mask bits equal to 32 • <dest-IP/Mask>|any|host <IP> – Defines the destination host IP address or destination network address • log – Generates log messages when a packet coming from an interface matches an ACL entry. Log messages are generated only for router ACLs • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • mark – Use with mark command to mark a packet • 8012p <0-7> – Sets the 802.1p VLAN user priority value to <vlan-priority-value> (0-7) • dscp <0-63> – Sets the Differentiated Services Code Point code-point value to <dscp-codepoint-value> (0-63)
permit icmp [<source-IP/ Mask>|any|host <ip>] [<dest-IP/Mask>|any| host <IP>] {<ICMP-type> {<ICMP-code>}} {log} {rule-precedence <1-5000>]} {mark [8021p <0-7>|dscp<0-63> rule-precedence <1-5000> {rule-description} <WORD>}	Use with the permit command to allow ICMP packets • deny – Permits ICMP packets • icmp – Specifies ICMP as the protocol • [<source-IP>|any|host <IP>] – The <source-IP> is the source IP address of the network or host (in dotted decimal format). • any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32

	• [<dest-IP>|any|host <IP>] – Defines the destination host IP address or destination network address • <ICMP-type> {<ICMP-code>} – Sets the ICMP type value <ICMP-type> from 0 to 255, and is valid only for ICMP. The ICMP code value <ICMP-code> is from 0 to 255, and is valid only for protocol type icmp • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • mark – Use with mark command to mark a packet • 8012p <0-7> – Sets the 802.1p VLAN user priority value to <vlan-priority-value> (0-7) • dscp <0-63> – Sets the Differentiated Services Code Point (DSCP) code-point value to <dscp-codepoint-value> (0-63)

permit [tcp|udp] [<source-ip/Mask>|any|host <IP>] {eq <source-port>|range <starting-source-port> <ending-source-port>} [<dest-IP/Mask>|any|host <IP>] {eq <source-port>} {range <starting-source-port> <ending-source-port>} {log} {rule-precedence <1-5000>}{mark [8021p <0-7>|dscp<0-63> rule-precedence <1-5000> {rule-description} <WORD>}	Use with the permit command to allow TCP or UDP packets • permit – Permits TCP/UDP packets • [tcp|udp] – Specifies TCP or UDP as the protocol • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format) • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for the exact source (A.B.C.D) and the source-mask bits equal to 32 • eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535 • range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers) • <dest-IP/Mask>|any|host <IP> – Defines the destination host IP address or destination network address • eq <source-port> {range <starting-source-port> <ending-source-port>|word|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|smtp|ssh|telnet|tftp|www} – Defines a specific destination port to match • range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535 • <1-65535> – Destination port • <WORD> – Displays any service name • bgp – Bgp port 179 • dns – DNS port 53 • ftp – Ftp-ctrl port 21 • ftp-data – Ftp-data port 20 • gopher – Gopher port 70 • https – HTTPS port 443 • ldap – LDAP port 389 • nntp – NNTP port 119 • ntp – NTP port 123 • pop3 – Pop3 port 110 • smtp – SMTP port 25 • ssh – SSH port 22 • telnet – Telnet port 23 • tftp – TFTP port 69 • www – HTTP port 80 • mark – Use with mark command to mark a packet • 8012p <0-7> – Sets the 802.1p VLAN user priority value to <vlan-priority-value> (0-7) • dscp <0-63> – Sets the Differentiated Services Code Point (DSCP) code-point value to <dscp-codepoint-value> (0-63)

permit proto [<0-254>|WORD|eigrp|gre| igmp|igp|ospf|vrrp] [<source-IP/Mask>|any|host <IP>][<dest-IP/Mask>|any|host <IP>] {log} {rule-description <WORD>|rule-precedence <1-5000>}	Use with the permit command to allow any protocol other than TCP, UDP or ICMP • 0-254] – Displays protocol number • <WORD> – Refers to any protocol name • eigrp – EIGRP protocol 88 • gre – GRE protocol 47 • igmp – IGMP protocol 2 • igp – IGP protocol 9 • ospf – OSPF protocol 89 • vrrp – VRRP protocol 112 • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching • <source-IP/Mask>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0 • host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32 • <dest-IP/mask>|any|host <IP> – Defines the destination host IP address or destination network address • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs • rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • rule-description <WORD> – Defines access-list entry name

Usage Guidelines

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list. The following protocols are supported:

- ip
- icmp
- icp
- udp
- proto

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed based on the ACL configuration.

- Filtering on TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny packets

- Selecting ICMP allows the filter of ICMP packets based on type and node.

NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet matching the entry sent to the console.

Example

```
rfs7000-37FABE(config-ip-acl-test)#permit icmp any any log rule-precedence 200
rfs7000-37FABE(config-ip-acl-test)#

rfs7000-37FABE(config-ip-acl-test)#permit ip 192.168.1.10/24 192.168.2.0/24
rule-precedence 40
rfs7000-37FABE(config-ip-acl-test)#

rfs7000-37FABE(config-ip-acl-test)# permit proto eigrp any any mark 8021p 2 rule-
precedence 2
rfs7000-37FABE(config-ip-acl-test)#
```

12.1.3 no

ip-access-list

Negates a command or sets its default

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [deny|permit]
```

Parameters

deny	Specifies packets to reject
permit	Specifies packets to forward

Usage Guidelines

```
Removes an access list control entry. Provide the rule-precedence value when
using the no command.
```

Example

```
rfs7000-37FABE(config-ip-acl-test)#no mark 8021p 5 tcp 192.168.2.0/24 any rule-
precedence 10

rfs7000-37FABE(config-ip-acl-test)#no permit ip any any rule-precedence 10

rfs7000-37FABE(config-ip-acl-test)#no deny icmp any any rule-precedence 10
```

12.1.4 write

ip-access-list

Writes the running configuration to memory or terminal

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
write [terminal|memory]
```

Parameters

terminal	Writes to a terminal
memory	Writes to memory

Example

```
rfs7000-37FABE(config-ip-acl-test)#write terminal
!
! Configuration of RFS7000 version 5.1.0.0-036D
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
 assignable-power-range 8 9
!
wlan-qos-policy default
!
radio-qos-policy default
!
aaa-policy default
!
association-acl-policy default
!
wips-policy default
!
hotspot-policy default
!
firewall ratelimit-trust policy default
!
management-policy default
 telnet
 http server
 ssh
!
!
firewall dos-attack policy default
!
firewall policy default
!
radius-server-policy default
```

```
!
mint-security-policy the_policy
!
role-policy default
!
device-discover-policy default
!
```

12.1.5 clrscr

ip-access-list

Clears the display screen

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clrscr
```

Parameters

None

Example

```
rfs7000-37FABE(config-ip-acl-test)#clrscr
rfs7000-37FABE(config-ip-acl-test)#
```

12.1.6 commit

ip-access-list

Commits all changes made in the current session

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`commit {write} {memory}`

Parameters

write	If a commit succeeds, the configuration is written to memory
memory	Writes to memory

Example

```
rfs7000-37FABE(config-ip-acl-test)#commit write memory
[OK]
rfs7000-37FABE(config-ip-acl-test)#
```

12.1.7 end

ip-access-list

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to the previous mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
end
```

Parameters

None

Example

```
rfs7000-37FABE(config-ip-acl-test)#end
rfs7000-37FABE#
```

12.1.8 exit

ip-access-list

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to the previous mode.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
exit
```

Parameters

None

Example

```
rfs7000-37FABE(config-ip-acl-test)#exit
rfs7000-37FABE(config-ip-acl-test)#
```

12.1.9 help

ip-access-list

Displays the interactive help system

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
help
```

Parameters

None

Example

```
rfs7000-37FABE(config-ip-acl-test)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup until entering a
'?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to
know what arguments match the input e.g. 'show ve?'.)
rfs7000-37FABE(config-ip-acl-test)#
```

12.1.10 revert

ip-access-list

Reverts any updates to their last saved configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
revert
```

Parameters

None

Example

```
rfs7000-37FABE(config-ip-acl-test)#revert
rfs7000-37FABE(config-ip-acl-test)#
```

12.1.11 service

ip-access-list

Displays service commands

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
service show cli
```

Parameters

show	Displays running system configuration
cli	Displays the CLI tree of the current mode

Example

```
rfs7000-37FABE(config-ip-acl-test)#service show cli
AAA Policy Mode mode:
+-help [help]
+-show
  +-commands [show commands]
  +-running-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config) (|include-factory)]
  +-session-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config) (|include-factory)]
  +-device
    +-DEVICE [show device DEVICE (|include-factory)]
      +-include-factory [show device DEVICE (|include-factory)]
  +-session-changes [show session-changes]
  +-internal
    +-context
      +-running-config
       +-WORD [show internal context (running-config|session-config) WORD (|include-
factory)]
          +-include-factory [show internal context (running-config|session-config)
WORD (|include-factory)]
      +-session-config
       +-WORD [show internal context (running-config|session-config) WORD (|include-
factory)]
          +-include-factory [show internal context (running-config|session-config)
WORD (|include-factory)]
  +-startup-config [show startup-config (|include-factory)]
    +-include-factory [show startup-config (|include--DOMAIN-NAME [show wireless
mobile-unit (|(on DEVICE-OR-DOMAIN-NAME))]
      +-mac
        +-AA-BB-CC-DD-EE-FF [show wireless mobile-unit mac AA-BB-CC-DD-EE-FF (|(on
DEVICE-OR-DOMAIN-NAME))]
          +-on
           +-DEVICE-OR-DOMAIN-NAME [show wireless mobile-unit mac AA-BB-CC-DD-EE-FF
(|(on DEVICE-OR-DOMAIN-NAME))]
      +-statistics [show wireless mobile-unit statistics (|traffic) (|(on DEVICE-OR-
DOMAIN-
```

```
NAME))].....................................................................
.......................
rfs7000-37FABE(config-ip-acl-test)#
```

12.1.12 show

ip-access-list

Displays running system information

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
show <parameter>
```

Parameters

None

Example

```
rfs7000-37FABE(config-ip-acl-test)#show ?
  aclstats          ACL stats
  adoption          Display information related to adoption
  advanced-wips     Advanced WIPS
  boot              Display boot configuration.
  clock             Display system clock
  commands          Show command lists
  context           Information about current context
  crypto            Encryption related commands
  debugging         Debugging functions
  device            Device configuration
  event-history     Display event history
  file              Display filesystem information
  firewall          Wireless Firewall
  hotspot           Hotspot functions
  interface         Interface Configuration/Statistics commands
  ip                Internet Protocol (IP)
  mint              MiNT protocol
  ntp               Network time protocol
  role              Role based firewall
  running-config    Current operating configuration
  session-changes   Configuration changes made in this        session
  session-config    This session configuration
  smart-rf          Smart-RF Management Commands
  startup-config    Startup configuration
  terminal          Display terminal configuration parameters
  upgrade-status    Display last image upgrade status
  version           Display software & hardware version
  wireless          Wireless commands
rfs7000-37FABE(config-ip-acl-test)#
```

12.2 mac-access-list

Table 12.2 Summarizes MAC Access list commands

Table 12.2 *mac-access-list Commands*

Command	Description	Reference
deny	Use this command to specify packets to reject	*page 12-35*
permit	Use this command to specify packets to accept	*page 12-28*

12.2.1 permit

mac-access-list

Specifies specific packets to forward

NOTE: Use a decimal value representation of ethertypes to implement a `permit/deny` designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

Supported in the following platforms:

- RFS 7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
permit[<source-MAC>|any|host]

permit <source-MAC> <AA-BB-CC-DD-EE-FF> <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p <0-
7>|log|mark [8021p<0-7>|dscp<0-63>[rule-precedence <1-5000>[rule-description
<WORD>]]|rule-precedence <1-5000>[rule-description <WORD>|type [8021q|<1-
65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log|rule-precedence <1-5000>
rule-desription <WORD>]|vlan <1-4095> [log|rule-precedence|type[8021q|
<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]

permit [any|host] <dest-MAC> <dest-mask> [dot1p <0-7>|log|mark [8021p<0-7>|dscp<0-
63>[rule-precedence <1-5000>[rule-description <WORD>]|rule-precedence <1-5000>[rule-
description <WORD>|type [8021q|<1-
65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log|rule-precedence]|vlan <1-
4095> [log|rule-precedence<1-5000> rule-desription <WORD>|type[8021q|
<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]]
```

Parameters

permit	Use with a permit command to allow IP packets
permit <source-MAC> <AA-BB-CC-DD-EE-FF> <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p <0-7>|log|mark [8021p<0-7>|dscp<0-63>[rule-precedence <1-5000> [rule-description <WORD>]]|rule-precedence <1-5000>[rule-description <WORD>|type [8021q|<1-65535>|aarp|appletalk| arp|ip|ipv6|ipx|mint|rarp|wisp] [log| rule-precedence <1-5000> rule-desription <WORD>]|vlan <1-4095> [log| rule-precedence|type[8021q| <1-65535>|aarp|appletalk |arp|ip|ipv6|ipx|mint|rarp|wisp]	• permit – Sets the ACL action type • <source-MAC> – Specify a source MAC address to match • <AA-BB-CC-DD-EE-FF> – Specify a source MAC address mask • <dest-MAC> – Defines the destination MAC address • any – any destination host • host – Defines the exact destination MAC address to match • <AA-BB-CC-DD-EE-FF> – Defines the source MAC address mask • dot1p <0-7> [log|rule-precedence|type] – 802.1p priority • <0-7> – Priority value • log – Generates log messages when the packet coming from the interface matches an ACL entry Log messages are generated only for router ACLs • mark [8021p<0-7>|dscp<0-63>[rule-precedence <1-5000>[rule-description <WORD>]] – Specifies packets to mark • 8021p <0-7> – Modifies 802.1p VLAN user priority. Select a VLAN user VLAN user priority value • dscp <0-63> – Sets the Differentiated Services Code Point (DSCP) code-point value to <dscp-codepoint-value> (0-63) • <0-63> – Specify a DSCP codepoint value from 0-63 • rule-precedence<1-5000>rule-description <WORD> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • rule-description – Access-list entry description • <WORD> – Specify the description up to 128 characters • type[8021q|<1-65535>|aarp|apple-talk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log <0-7>| rule-precedence <1-5000>] – Ether Type • 8021q – VLAN Ether Type (0x8100) • <1-65535> – Ethernet protocol number

	• aarp – AARP Ether Type (0x80F3) • appletalk – APPLETALK Ether Type (0x809B) • arp – ARP Ether Type (0x0806) • ip – IP Ether Type (0x0800) • ipv6 – IPv6 Ether Type (0x86DD) • ipx – IPX Ether Type (0x8137) • mint – MINT Ether Type (0x8783) • rarp – RARP Ether Type (0x8035) • wisp –WISP Ether Type (0x8783) • vlan <1-4095> [log|rule-precedence <1-5000> rule-desription <WORD>|type] – VLAN ID • <1-4095> – Specify a VLAN ID between 1-4095

any <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p <0-7>|log|mark [8021p<0-7>|dscp<0-63>[rule-precedence <1-5000> [rule-description <WORD>]] rule-precedence <1-5000> [rule-description <WORD>|type [8021q|<1-65535>|aarp|appletalk| arp|ip|ipv6|ipx|mint|rarp|wisp] [log|rule-precedence]|vlan <1-4095> [log|rule-precedence|type[8021q| <1-65535>|aarp|appletalk| arp|ip|ipv6|ipx|mint|rarp|wisp]	any – Specify any source host to match • <dest-MAC> – Defines the destination MAC address • <AA-BB-CC-DD-EE-FF> – Defines the destination MAC address mask to match • host – Defines exact destination MAC address to match • AA-BB-CC-DD-EE-FF – Defines the source MAC address mask • dot1p <0-7> [log|rule-precedence|type] – 802.1p priority • <0-7> – priority value • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs • mark [8021p<0-7>|dscp<0-63>[rule-precedence <1-5000>[rule-description <WORD>]] – Use with mark command to mark a packet • 8021p <0-7> – Modifies 802.1p VLAN user priority. Select a VLAN user priority value • dscp <0-63> – Sets the differentiated services code-point value to <dscp-codepoint-value> (0-63) • <0-63> – Specify a DSCP codepoint value from 0-63 • rule-precedence <1-5000> rule-description <WORD> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • rule-description – Access-list entry description • <WORD> – Specify the description not exceeding 128 characters • type[8021q|<1-65535>|aarp|apple-talk|arp|ip|ipv6|ipx|mint|rarp|wisp][log<0-7>| rule-precedence <1-5000>] – Ether Type • 8021q – VLAN Ether Type (0x8100) • <1-65535> – Ethernet Protocol number • aarp – AARP Ether Type (0x80F3) • appletalk – APPLETALK Ether Type (0x809B) • arp – ARP Ether Type (0x0806) • ip – IP Ether Type (0x0800) • ipv6 – IPv6 Ether Type (0x86DD) • ipx – IPX Ether Type (0x8137) • mint – MINT Ether Type (0x8783) • rarp – RARP Ether Type (0x8035) • wisp –WISP Ether Type (0x8783)
	• vlan <1-4095> [log|rule-precedence <1-5000> rule-desription <WORD>|type – VLAN ID • <1-4095> – Specify a VLAN ID between 1-4095

host <source-MAC> <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p <0-7>|log|mark [8021p<0-7>|dscp<0-63>[rule-precedence <1-5000>[rule-description <WORD>]]|rule-precedence <1-5000>[rule-description <WORD>|type [8021q|<1-65535>|aarp| appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]] [log|mark|rule-precedence]	Defines exact source address to match • <source-MAC> – Defines source MAC address to match • <dest-MAC> – Defines destination MAC address to match • <AA-BB-CC-DD-EE-FF> – Defines destination MAC address mask to match • dot1p <0-7> [log|rule-precedence|type] – 802.1p priority • <0-7> – priority value • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs • mark [8021p<0-7>|dscp<0-63>[rule-precedence <1-5000>[rule-description <WORD> – Specifies packets to mark • dscp <0-63> – Sets the Differentiated Services Code Point (DSCP) code-point value to <dscp-codepoint-value> (0-63) • <0-63> – Specify a DSCP codepoint value from 0-63 • 8021p <0-7> – Modifies 802.1p VLAN user priority. Select a VLAN user VLAN user priority value • rule-precedence<1-5000>rule-description <WORD> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • rule-description – Access-list entry description

	• <WORD> – Specify the description not exceeding 128 characters
	• rule-precedence <1-5000> rule-description <WORD> – Defines an integer value between 1-5000 to set the rule precedence in the ACL • rule-description – Access-list entry description • <WORD> – Specify the description not exceeding 128 characters • type[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log <0-7>|rule-precedence <1-5000>][log|mark|rule-precedence] – Ether Type • 8021q – VLAN Ether Type (0x8100) • <1-65535> – Ethernet protocol number • aarp – AARP Ether Type (0x80F3) • appletalk – APPLETALK Ether Type (0x809B) • arp – ARP Ether Type (0x0806) • ip – IP Ether Type (0x0800) • ipv6 – IPv6 Ether Type (0x86DD) • ipx – IPX Ether Type (0x8137) • mint – MiNT Ether Type (0x8783) • rarp – RARP Ether Type (0x8035) • wisp –WISP Ether Type (0x8783) • vlan <1-4095> [log|rule-precedence <1-5000> rule-desription <WORD>|type] – VLAN ID • <1-4095> – Specify a VLAN ID value between 1-4095

The following parameters are common for all the 'Ethertype' parameters:

log	Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs
mark [8021p<0-7>|dscp <0-63>[rule-precedence <1-5000>[rule-description <WORD>	Specifies packets to mark
rule-precedence <1-5000> rule-description <WORD>	Defines an integer value between 1-5000. This value sets the rule precedence in the ACL

Usage Guidelines

The permit command in the MAC ACL disallows traffic based on layer 2 (data-link layer) information. A MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, or ethernet type. Common types include:

- arp
- wisp
- ip
- 802.1q

The controller (by default) does not allow layer 2 traffic to pass through the interface. To adopt an access point through an interface, configure an access control list to allow an Ethernet WISP

Use the mark option to specify the type of service (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is marked based on the ACL's configuration

NOTE: To apply an IP based ACL to an interface, a MAC access list entry is mandatory to allow ARP. A MAC ACL always takes precedence over IP based ACLs.

Example

```
rfs7000-37FABE(config-mac-acl-test)#permit any any vlan 2 log rule-precedence 5 rule-
description testrule
rfs7000-37FABE(config-mac-acl-test)#
```

12.2.2 deny

mac-access-list

Specifies packets to reject

NOTE: Use a decimal value representation of ethertypes to implement a `permit/deny` designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
deny[<source-MAC>|any|host]

deny <source-MAC> <AA-BB-CC-DD-EE-FF> <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p <0-
7>|log|rule-precedence <1-5000>[rule-description <WORD>|type [8021q|<1-
65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log|rule-precedence <1-5000>
rule-desription <WORD>]|vlan <1-4095> [log|rule-precedence|type[8021q|<1-
65535>|aarp|appletalk|arp|ip|
ipv6|ipx|mint|rarp|wisp]]

deny [any|host] <dest-MAC> <dest-mask> [dot1p <0-7>|log|rule-precedence <1-
5000>[rule-description <WORD>|type [8021q|<1-65535>|aarp|appletalk|
arp|ip|ipv6|ipx|mint|rarp|wisp] [log|rule-precedence]|vlan <1-4095> [log|rule-
precedence<1-5000> rule-desription <WORD>|type[8021q|<1-65535>|aarp|appletalk|
arp|ip|ipv6|ipx|mint|rarp|wisp]]
```

Parameters

deny	Use with the deny command to reject packets
deny [<source-MAC>|any|host	• deny – Sets the action type on a ACL • <source-MAC> – Specify the source MAC address • <AA-BB-CC-DD-EE-FF> – Specify the source MAC address mask • <dest-MAC> – Specify the destination MAC address • any – any destination host • host – host is an abbreviation for the exact source <MAC Address> (AA-BB-CC-DD-EE-FF format) and source-mask bits equal to 32 • AA-BB-CC-DD-EE-FF – Specify the source MAC address mask • dot1p <0-7> [log|rule-precedence|type] – Sets the 802.1p priority value • <0-7> – Set the priority value from 0-7 • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence<1-5000>rule-description <WORD> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • <1-5000> – Specify a precedence value from 1-5000 • rule-description – Access-list entry description • <WORD> – Enter the description not exceeding 128 characters • type[8021q|<1-65535>|aarp|apple-talk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log <0-7>| rule-precedence <1-5000>] – Specifies various Ether types • 8021q – VLAN Ether Type (0x8100) • <1-65535> – Ethernet Protocol number • aarp – AARP Ether Type (0x80F3) • appletalk – APPLETALK Ether Type (0x809B) • arp – ARP Ether Type (0x0806) • ip – IP Ether Type (0x0800) • ipv6 – IPv6 Ether Type (0x86DD) • ipx – IPX Ether Type (0x8137) • mint – MINT Ether Type (0x8783) • rarp – RARP Ether Type (0x8035) • wisp –WISP Ether Type (0x8783) • vlan <1-4095> [log|rule-precedence <1-5000> rule-desription <WORD>|type – VLAN ID • <1-4095> – Specify a VLAN ID from 1-4095

any <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p <0-7>|log|rule-precedence <1-5000>[rule-description <WORD>|type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log|rule-precedence]|vlan <1-4095> [log|rule-precedence|type[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]	any <dest-MAC> –Specify a destination MAC address • <AA-BB-CC-DD-EE-FF> – Specify any destination MAC address mask • dot1p <0-7> – Sets the 802.1p priority value from 0-7 • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence<1-5000>rule-description <WORD> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • rule-description – Access-list entry description • <WORD> – Enter the description not exceeding 128 characters • type[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log <0-7>|rule-precedence <1-5000>] – Specify the EtherType • 8021q – VLAN Ether Type (0x8100) • <1-65535> – Ethernet Protocol number • aarp – AARP Ether Type (0x80F3) • appletalk – APPLETALK Ether Type (0x809B) • arp – ARP Ether Type (0x0806) • ip – IP Ether Type (0x0800) • ipv6 – IPv6 Ether Type (0x86DD) • ipx – IPX Ether Type (0x8137) • mint – MiNT Ether Type (0x8783) • rarp – RARP Ether Type (0x8035) • wisp – WISP Ether Type (0x8783) • vlan <1-4095> [log|rule-precedence <1-5000> rule-desription <WORD>|type] – VLAN ID • <1-4095> – Specify a VLAN ID from 1-4095

host <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p <0-7>|log|rule-precedence <1-5000>[rule-description <WORD>|type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log|rule-precedence]|vlan <1-4095> [log|rule-precedence|type[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]	host – Specify an exact source MAC address to match • <dest-MAC> – Specify the destination MAC address • dot1p <0-7> – Sets the 802.1p priority value from 0-7 • log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs. • rule-precedence<1-5000>rule-description <WORD> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL • <1-5000> – Specify a precedence value from 1-5000 • rule-description – Access-list entry description • <WORD> – Enter the description not exceeding 128 characters • type[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp] [log <0-7>| rule-precedence <1-5000>] – Specify the EtherType • 8021q – VLAN Ether Type (0x8100) • <1-65535> – Ethernet Protocol number • aarp – AARP Ether Type (0x80F3) • appletalk – APPLETALK Ether Type (0x809B) • arp – ARP Ether Type (0x0806) • ip – IP Ether Type (0x0800) • ipv6 – IPv6 Ether Type (0x86DD) • ipx – IPX Ether Type (0x8137) • mint – MINT Ether Type (0x8783) • rarp – RARP Ether Type (0x8035) • wisp –WISP Ether Type (0x8783) • vlan <1-4095> [log|rule-precedence <1-5000> rule-desription <WORD>|type – VLAN ID • <1-4095> – Specify a VLAN ID from 1-4095

Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) data. The MAC access list denies traffic from a particular source MAC address or any MAC address. It can also disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can disallow traffic based on the VLAN and ethertype.

- arp
- wisp
- ip
- 802.1q

NOTE: MAC ACLs always takes precedence over IP based ACLs.

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL's configuration.

Example

```
rfs7000-37FABE(config-mac-acl-test)#deny 41-85-45-89-66-77 44-22-55-88-77-99 any vlan
1 log rule-precedence 2 rule-description test
rfs7000-37FABE(config-mac-acl-test)#
```

The MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
rfs7000-37FABE(config-mac-acl-test)#deny any host 00:01:ae:00:22:11
rfs7000-37FABE(config-mac-acl-test)#
```

The example below denies traffic between two hosts based on MAC addresses:

```
rfs7000-37FABE(config-mac-acl-test)#deny host 01:02:fe:45:76:89 host
01:02:89:78:78:45
rfs7000-37FABE(config-mac-acl-test)#
```

CHAPTER 13 DHCP-SERVER-POLICY

This chapter summarizes DHCP Server Policy commands within CLI structure.

Use the (config) instance to configure DHCP Server Policy related configuration commands. To navigate to the dhcp-server-policy instance, use the following commands:

```
rfs7000-37FABE(config)#dhcp-server-policy <policy-name>
rfs7000-37FABE(config)#dhcp-server-policy test
rfs7000-37FABE(config-dhcp-server-policy-test)#
rfs7000-37FABE(config-dhcp-policy-test)#?
DHCP policy Mode commands:
  bootp        BOOTP specific configuration
  dhcp-class   Configure DHCP Server class
  dhcp-pool    Configure DHCP server address pool
  no           Negate a command or set its defaults
  option       Define DHCP server option
  ping         Specify ping parameters used by DHCP Server

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write       Write running configuration to memory or terminal
rfs7000-37FABE(config-dhcp-policy-test)#
```

13.1 dhcp-server-policy

Table 13.1Summarizes dhcp-server-policy commands

Table 13.1 *dhcp-server-policy Commands*

Command	Description	Reference
bootp	Configures a BOOTP specific configuration	*page 13-3*
dhcp-pool	Configures a DHCP server address pool	*page 13-4*
option	Defines the DHCP option used in DHCP pools	*page 13-38*
no	Negates a command or sets its default value	*page 13-39*
ping	Specifies ping parameters used by a DHCP server	*page 13-40*
dhcp-class	Configures a DHCP server class	*page 13-41*

13.1.1 bootp

dhcp-server-policy

Configures a BOOTP specific configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
bootp ignore
```

Parameters

bootp ignore	Configures a BOOTP specific configuration • ignore – Configures a DHCP server to ignore BOOTP requests

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#bootp ignore
rfs7000-37FABE(config-dhcp-policy-test)#
```

13.1.2 dhcp-pool

dhcp-server-policy

Configures a DHCP server address pool

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rfs7000-37FABE(config-dhcp-policy-test)#dhcp-pool pool1
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

Parameters

<WORD>	Specify a pool name

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#?
DHCP pool Mode commands:
  address               Configure network pool's include address
  bootfile              Boot file name
  ddns                  Dynamic DNS Configuration
  default-router        Default routers
  dns-server            DNS Servers
  domain-name           Configure domain-name
  excluded-address      Prevent DHCP Server from assigning certain addresses
  lease                 Address lease time
  netbios-name-server   NetBIOS (WINS) name servers
  netbios-node-type     NetBIOS node type
  network               Network on which DHCP server will be deployed
  next-server           Next server in boot process
  no                    Negate a command or set its defaults
  option                Raw DHCP options
  respond-via-unicast   Send DHCP offer and DHCP Ack as unicast messages
  static-binding        Configure static address bindings
  static-route          Add static routes to be installed on dhcp clients
  update                Control the usage of DDNS service

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal
```

13.1.3 dhcp-pool-mode

Configures dhcp-pool commands

Table 13.2 Summarizes dhcp-pool commands

Table 13.2 *dhcp-pool-mode Commands*

Command	Description	Reference
address	Specifies a range of addresses for a DHCP network pool	*page 13-6*
bootfile	Assigns a bootfile name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted	*page 13-7*
ddns	Configures dynamic DNS parameters	*page 13-8*
default-router	Configures a default-router or gateway IP address for the network pool	*page 13-9*
dns-server	Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool	*page 13-10*
domain-name	Sets the domain name for the network pool	*page 13-11*
excluded-address	Prevents a DHCP server from assigning certain addresses to the DHCP pool	*page 13-12*
lease	Sets a valid lease time for the IP address used by DHCP clients in the DHCP pool	*page 13-13*
netbios-name-server	Configures NetBIOS (WINS) name server IP address	*page 13-15*
netbios-node-type	Defines the NetBIOS node type	*page 13-16*
next-server	Configures the next server in the boot process	*page 13-17*
no	Negates a command or sets its default value	*page 13-18*
option	Configures RAW DHCP options	*page 13-19*
respond-via-unicast	Sends a DHCP offer and a DHCP Ack as unicast messages	*page 13-20*
update	Controls the usage of DDNS service	*page 13-21*
static-binding	Configures static address bindings	*page 13-22*

13.1.3.1 address

dhcp-pool-mode

Specifies a range of addresses for the DHCP network pool

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
address [address {class} <DHCP-CLASS>|range <Low IP> <High IP>{class}
<DHCP-CLASS>]
```

Parameters

[address {class} <DHCP-CLASS>|range <Low IP> <High IP>{class} <DHCP-CLASS>]	• address – Specify the address to include in the network pool
	• range – Adds an address range for the DHCP server
	  • <Low IP> – Defines the first IP address in the address range
	  • <High IP> – Defines the last IP address in the address range
	The following parameters are common for both the address and range
	  • class – Specify the DHCP class name to which the address range is attached
	  • <DHCP-CLASS> – Specify the name of the DHCP class

Usage Guidelines

Use the `no address range` command to remove the DHCP address range.

Use the address command to specify a range of addresses for the DHCP network pool. The DHCP server assigns IP address to DHCP clients from the address range. A high IP address is the upper limit for providing the IP address, and a low IP address is the lower limit for providing the IP address.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#address range 1.2.3.4
5.6.7.8 class dhcp1
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#address 1.2.3.4 class
dhcp1
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.2 bootfile

dhcp-pool-mode

Assigns a bootfile name for the DHCP configuration in the network pool

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
bootfile <WORD>
```

Parameters

<WORD>	Sets the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted

Usage Guidelines

Use the `bootfile` command to specify the boot image. The boot file contains the boot image name used for booting the bootp clients (DHCP clients). Only one boot file is allowed per pool.

Use `{no} bootfile` command to remove the bootfile. Do not use the <file name> with the bootfile command as only one bootfile exists per pool. The command `[no]bootfile` removes the existing command from the pool.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#bootfile test.txt
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.3 ddns

dhcp-pool-mode

Configures dynamic DNS parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ddns [domain-name <WORD>|multiple-userclass|server <A.B.C.D> {A.B.C.D}|ttl
<1-864000>]
```

Parameters

domain-name <WORD>	Sets the domain name used for DDNS updates
multiple-userclass	Enables multiple user class option
server <A.B.C.D> {A.B.C.D}	Specify the server IP address to which DDNS updates have been sent • <A.B.C.D> – Defines an IP address in dotted decimal format
ttl <1-864000>	Select a *Time To Live* (TTL) value between 1 and 864000 for DDNS updates

Usage Guidelines

Use `update dns override` to enable an internal DHCP server to send DDNS updates for resource records (RRs) A, TXT and PTR. A DHCP server can always override the client even if the client is configured to perform the updates.

In the DHCP server network pool, FQDN is defined as the DDNS domain name. This is used internally in DHCP packets between the DHCP server on the controller and the DNS server.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#ddns domainname WID
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#ddns multiple-user-
class
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#ddns server 172.16.10.9
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.4 default-router

dhcp-pool-mode

Configures a default-router or gateway IP address for the network pool. To remove the default router list, use the no default-router command.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
default-router <A.B.C.D> {<A.B.C.D>}
```

Parameters

<A.B.C.D> {<A.B.C.D>}	Specifies the default router IP address for the network pool. The maximum number of IP's that can be configured is 8.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#default-router
172.16.10.8 172.16.10.9
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.5 dns-server

dhcp-pool-mode

Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool. Use the no dns-server command to remove the DNS server list.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dns-server <A.B.C.D>
```

Parameters

<A.B.C.D>	Configures the DNS server's IP address • <A.B.C.D> – Sets the server's IP address. Up to 8 IPs can be set

Usage Guidelines

For DHCP clients, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#dns-server 172.16.10.7
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.6 domain-name

dhcp-pool-mode

Sets the domain name for the DHCP pool. Use the `no domain-name` command to remove the domain name.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
domain-name <WORD>
```

Parameters

<WORD>	Defines the domain name for the DHCP pool

Usage Guidelines

For DHCP clients, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#domain-name
documentation
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.7 excluded-address

dhcp-pool-mode

Prevents a DHCP Server from assigning certain addresses to the DHCP pool

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
excluded-address [<A.B.C.D>|range <Low IP> <High IP>]
```

Parameters

[<A.B.C.D>|range <Low IP> <High IP>]	• <A.B.C.D> – Specify the IP address to exclude or low IP address in a range • range – Specify a range of excluded addresses from the DHCP pool • <Low IP> – Specify the low IP address to exclude • <High IP> – Specify the high IP address to exclude These IP addresses are excluded by the DHCP server when assigning IP address to servers

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#excluded-address 172.16.10.9
172.16.10.10
rfs7000-37FABE(config-dhcp-policy-test)#
```

13.1.3.8 lease

dhcp-pool-mode

Sets a valid lease time for the IP address used by DHCP clients in the DHCP pool

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
lease [<0-365> {0-23} {0-59> {0-59}|infinite]
```

Parameters

<0-365>	Select a value between 0 and 365 days to configure lease time. Days may be 0 only when hours and/or mins are greater than 0 • <0-23> – Sets the lease period in hours. Hours can be 0 only when days and/or minutes are configured with a value greater than 0 • <0-59> – Sets the lease period in minutes. Minutes can be 0 only when days and/or hours are configured with a value greater than 0 • <0-59> – Sets the lease period in seconds
infinite	Sets the lease time as infinite

Usage Guidelines

If lease parameter is not configured on the DHCP pool, the default value is used. The default value of the lease is 24 hours.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#lease 1 0 0
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)# show running-config
include-factory
.....................................
ip dhcp pool Test4lease
 lease 1 0 0
 no domain-name
 no bootfile
 no dns-server
 no default-router
 no next-server
 no netbios-name-server
 no netbios-node-type
 no unicast-enable
 no update dns
 no ddns domainname
 no ddns ttl
 no ddns multiple-user-class
```

```
 client-name test4lease
 client-identifier tested4lease
.............................................................
.......................................
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1))#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#lease infinite
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.9 netbios-name-server

dhcp-pool-mode

Configures the NetBIOS (WINS) name server IP address

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
netbios-name-server <A.B.C.D>
```

Parameters

<A.B.C.D>	Sets the NetBIOS name server's IP address

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#netbios-name-server
172.16.10.23
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.10 netbios-node-type

dhcp-pool-mode Commands

Defines the netbios-node-type

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
netbios-node-type [b-node|h-mode|m-node|p-node]
```

Parameters

[b-node|h-mode| m-node|p-node]	Defines the netbios-node-type • b-node – The type is broadcast node • h-node – The type is hybrid node • m-node – The type is mixed node • p-node – The type is peer-to-peer node

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#netbios-node-type
b-node
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.11 next-server

dhcp-pool-mode

Configures the next server in the boot process

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
next-server <A.B.C.D>
```

Parameters

<A.B.C.D>	Configures the IP address of the next server in the boot process

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#next-server
172.16.10.24
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.12 no

dhcp-pool-mode

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [address|bootfile|ddns|default-router|dns-server|domain-name|
excluded-address|lease|netbios-name-server|netbios-node-type|network|
next-server|option|respond-via-unicast|static-binding|static-route|update]
```

Parameters

[address|bootfile|ddns| default-router|dns-server|domain-name|excluded-address| lease|netbios-name-server|netbios-node-type|network| next-server|option|respond-via-unicast| static-binding| static-route|update]	• address – Unconfigures network pool's include addresses • bootfile – Specifies a boot file name • default-router – Unconfigures the default router • dns-server – Unconfigures the DNS server • domain-name – Unconfigures the domain name • excluded-address – Prevents a DHCP server from assigning certain addresses • lease – Disables an address lease time • netbios-name-server – Unconfigures NetBIOS (WINS) name server • netbios-node-type – Unconfigures NetBIOS node type • next-server – Unconfigures the next server in the boot process • option – Raw DHCP options • respond-via-unicast – Sends a DHCP offer and DHCP Ack as broadcast messages • static-binding – Removes static address bindings • static-route – Adds static routes installed on DHCP clients • update – Controls the usage of DDNS service

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no bootfile
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no network
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no lease
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#no default-router
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.13 option

dhcp-pool-mode

Configures raw DHCP options. The DHCP option has to be configured under the DHCP-Server-Policy. The options configured under the DHCP-Pool/DHCP-Server-Policy can also be used in static-bindings.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
option <option-name> [<A.B.C.D>|<WORD>]
```

Parameters

<option-name>	Specify the name of the DHCP option to configure
<A.B.C.D>	Sets the IP value of the DHCP option
<WORD>	Sets the ASCII value of the DHCP option

Usage Guidelines

Defines non standard DHCP option codes (0-254)

NOTE: An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use `show runnig config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#option option1
157.235.208.80
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.3.14 respond-via-unicast

dhcp-pool-mode

Sends a DHCP offer and a DHCP Ack as unicast messages

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131
- AP650
- AP6511
- AP6532

Syntax

```
respond-via-unicast
```

Parameters

None

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#respond-via-unicast
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

NOTE: The commands clrscr, commit, exit, help, show, service, revert, write are common commands. Refer to *Chapter 5, COMMON COMMANDS* for more information.

13.1.3.15 update

dhcp-pool-mode

Controls the usage of the DDNS service

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`update dns {override}`

Parameters

dns {override}	Dynamic DNS Configuration • override – Enables dynamic updates by onboard DHCP Server

Usage Guidelines

A DHCP client cannot perform updates for RR's A, TXT and PTR. Use `update (dns)(override)` to enable the controller's internal DHCP server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP Server can override the client, even if the client is configured to perform the updates.

In the DHCP pool of DHCP server, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the controller's DHCP server and the DNS server.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#update dns override
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

13.1.4 static-binding

dhcp-pool-mode

Configures static address bindings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
static-binding [client-identifier <WORD>|hardware-address <AA-BB-CC-DD-EE-FF>]
```

Parameters

[client-identifier <WORD>|hardware-address <AA-BB-CC-DD-EE-FF>]	• client-identifier <WORD> – Specify the client identifier for the DHCP client (DHCP option 61) • <WORD> – ASCII string. To prepend null character use \\0 at beginning. Single \ in the input will be ignored. • hardware-address <AA-BB-CC-DD-EE-FF> – Specify the hardware address of the DHCP client

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#static-binding client-
identifier Hex
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-Hex)#?
DHCP static binding Mode commands:
  bootfile              Boot file name
  client-name           Client name
  default-router        Default routers
  dns-server            DNS Servers
  domain-name           Configure domain-name
  ip-address            Fixed IP address for host
  netbios-name-server   NetBIOS (WINS) name servers
  netbios-node-type     NetBIOS node type
  next-server           Next server in boot process
  no                    Negate a command or set its defaults
  option                Raw DHCP options
  respond-via-unicast   Send DHCP offer and DHCP Ack as unicast messages
  static-route          Add static routes to be installed on dhcp clients

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal
```

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-Hex)#

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-
66)#?
DHCP static binding Mode commands:
  bootfile              Boot file name
  client-name           Client name
  default-router        Default routers
  dns-server            DNS Servers
  domain-name           Configure domain-name
  ip-address            Fixed IP address for host
  netbios-name-server   NetBIOS (WINS) name servers
  netbios-node-type     NetBIOS node type
  next-server           Next server in boot process
  no                    Negate a command or set its defaults
  option                Raw DHCP options
  respond-via-unicast   Send DHCP offer and DHCP Ack as unicast messages
  static-route          Add static routes to be installed on dhcp clients

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-
66)#
```

13.1.5 static-binding-mode

Use the (config) instance to configure `dhcp-static-binding` related configuration commands. To navigate to the instance, use the following commands:

```
rrfs7000-37FABE(config-dhcp-policy-test-pool-pool1)#static-binding client-identifier Hex
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-Hex)#?
```

Table 13.3 Summarizes static-binding-mode commands

Table 13.3 *static-binding Commands*

Command	Description	Reference
bootfile	Assigns a bootfile name for the DHCP configuration on the network pool	*page 13-25*
client-name	Specifies a client-name to configure	*page 13-26*
default-router	Configures default-router or gateway IP address for the network pool	*page 13-27*
dns-server	Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool	*page 13-28*
domain-name	Sets the domain name for the network pool	*page 13-29*
ip-address	Configures a fixed IP address for a host	*page 13-30*
netbios-name-server	Configures a NetBIOS (WINS) name server IP address	*page 13-31*
netbios-node-type	Defines the NetBIOS node type	*page 13-32*
next-server	Configures the next-server in the boot process	*page 13-33*
no	Negates a command or sets its default value	*page 13-34*
option	Configures raw DHCP options	*page 13-35*
respond-via-unicast	Sends a DHCP offer and DHCP Ack as unicast messages	*page 13-20*
static-route	Adds static routes to be installed on DHCP clients	*page 13-37*

13.1.5.1 bootfile

static-binding-mode

Specifies a bootfile name for the DHCP configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
bootfile <WORD>
```

Parameters

<WORD>	Specify a boot file name. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Usage Guidelines

Use the bootfile command to specify the boot image. The boot file contains the boot image name used for booting the BOOTP clients (DHCP clients). Only one boot file is allowed per pool.

Use {no} bootfile command to remove the bootfile. Do not use the <file name> with the bootfile command as only one bootfile exists per pool. The command [no] bootfile removes the existing command from the pool.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#bootfile
test.txt
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#
```

13.1.5.2 client-name

static-binding-mode

Specifies a client-name

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
client-name <WORD>
```

Parameters

<WORD>	Specify a client-name to configure

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#client-name
RFID
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#
```

13.1.5.3 default-router

static-binding-mode

Configures the default router or gateway IP address for the network pool. To remove the default router list, use the no default-router command.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
default-router <A.B.C.D> {A.B.C.D}
```

Parameters

<A.B.C.D> {A.B.C.D}	Specify an IP address to configure a default router. The maximum number of IPs that can be configured is 8.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Example

```
rfs7000-37FABE(config-dhcp-net-pool-test)#default-router 157.235.208.246
157.235.208.247
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#show context
 network-pool nw
  default-router 157.235.208.246 157.235.208.247
```

13.1.5.4 dns-server

static-binding-mode

Sets the DNS server's IP address available to all DHCP clients connected to the pool. Use the no dns-server command to remove the DNS server list.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dns-server <A.B.C.D>
```

Parameters

<A.B.C.D>	Specify a static IP address to configure a DNS server. Up to 8 IPs can be set.

Usage Guidelines

For DHCP clients, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based in the order (sequence) configured.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#dns-server
172.16.10.7
rfs7000-37FABE(config-dhcp-net-pool-test)#
```

13.1.5.5 domain-name

static-binding-mode

Configures a domain name

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
domain-name <WORD>
```

Parameters

<WORD>	Specify a name for the domain

Usage Guidelines

The domain name cannot exceed 256 characters.

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#domain-name
Technicaldocumentation
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#
```

13.1.5.6 ip-address

static-binding-mode

Configures a fixed IP address for a host

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip-address <A.B.C.D>
```

Parameters

<A.B.C.D>	Configures a fixed IP address in dotted decimal format for the host

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#ip-address
172.16.10.9
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#
```

13.1.5.7 netbios-name-server

static-binding-mode

Configures a NetBIOS (WINS) name server's IP address

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
netbios-name-server <A.B.C.D>
```

Parameters

<A.B.C.D>	Sets the NetBIOS name server's IP address

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#netbios-
name-server 172.16.10.27
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#
```

13.1.5.8 netbios-node-type

static-binding-mode

Assigns a netbios-node-type from the list

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
netbios-node-type [b-node|h-mode|m-node|p-node]]
```

Parameters

[b-node|h-mode| m-node|p-node]	Defines the NetBIOS (WINS) name servers from the list • b-node – The type is broadcast node • h-node – The type is hybrid node • m-node – The type is mixed node • p-node – The type is peer-to-peer node

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#netbios-
node-type p-node
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#
```

13.1.5.9 next-server

static-binding-mode

Configures the next-server in the boot process

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
next-server <A.B.C.D>
```

Parameters

<A.B.C.D>	Configures the IP address of the next-server in the boot process

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#next-server
172.16.10.30
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1))#
```

13.1.5.10 no

static-binding-mode

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [bootfile|client-name||default-router|dns-server|
domain-name|ip-address||netbios-name-server|netbios-node-type|
next-server|option|respond-via-unicast|static-route]
```

Parameters

[bootfile|client-name||default-router|dns-server|domain-name|ip-address||netbios-name-server|netbios-node-type|next-server|option|respond-via-unicast|static-route]	• bootfile – Specifies a boot file name • client-name – Removes a client-name • default-router – Configures a default router • dns-server – Configures a DNS server • domain-name – Configures a domain name • ip-address – Disables a fixed IP address for the host • netbios-name-server – Configures a NetBIOS (WINS) name server • netbios-node-type – Configures a NetBIOS node type • next-server – Configures a next server in boot process • option – Raw DHCP options • respond-via-unicast – Sends a DHCP offer and DHCP Ack as broadcast messages • static-route – Removes static routes installed on DHCP clients

Example

```
rfs7000-37FABE(config-dhcp-net-pool-test)#no bootfile
rfs7000-37FABE(config-dhcp-net-pool-test)#
```

13.1.5.11 option

static-binding-mode

Configures raw DHCP options. The DHCP option has to be configured under DHCP-Policy. The options configured under DHCP-Server-Policy only can be used in static-bindings.

```
rfs7000-37FABE(config-dhcp-policy-test)#option test1  2 ascii
rfs7000-37FABE(config-dhcp-policy-test)#
```

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131
- AP650
- AP6511
- AP6532

Syntax

```
option [<A.B.C.D>|<WORD>]
```

Parameters

<A.B.C.D>	Sets the IP value of the DHCP option
<WORD>	Sets the ASCII value of the DHCP option

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-ascii)#option
option1 172.16.10.10
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-ascii)#
```

13.1.5.12 respond-via-unicast

static-binding-mode

Sends a DHCP offer and a DHCP Acknowledge as unicast messages

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
respond-via-unicast
```

Parameters

None

Example

```
rfs7000-37FABE(config-dhcp-net-pool-test)#respond-via-unicast
rfs7000-37FABE(config-dhcp-net-pool-test)#
```

13.1.5.13 static-route

static-binding-mode

Adds static routes to be installed on the DHCP clients

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
static-route  <A.B.C.D/M> <A.B.C.D>
```

Parameters

<A.B.C.D/M>	Enter the network number and mask to configure the subnet

Example

```
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#static-route
10.0.0.0/10  157.235.208.235
rfs7000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#?
```

NOTE: The commands clrscr, commit, exit, help, write, revert, service and show are common commands. For more information, see *Chapter 5, COMMON COMMANDS*.

13.1.6 option

dhcp-server-policy

Defines the DHCP option used in DHCP pools

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
option <WORD> <0-254> [ascii|ip]
```

Parameters

<WORD> <0-254>	Sets raw DHCP options
	• <0-254> – Enter an option code between 0 and 254
	  • ascii – Sets the ASCII value of the DHCP option
	  • ip – Sets the IP value of the DHCP option

Usage Guidelines

Defines non standard DHCP option codes (0-254)

NOTE: An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output (use `show runnig config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#option test1 2 ascii
rfs7000-37FABE(config-dhcp-policy-test)#

rfs7000-37FABE(config-dhcp-policy-test)#option test1 2 ip
rfs7000-37FABE(config-dhcp-policy-test)#
```

13.1.7 no

dhcp-server-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [bootp|excluded-address|host-pool|network-pool|option|ping]
```

Parameters

[bootp| excluded-address| host-pool| network-pool| option|ping]	• bootp – Unconfigures BOOTP specific configuration • excluded-address – Prevents a DHCP server from assigning certain addresses • host-pool – Deletes the DHCP server host address pool • network-pool – Deletes the DHCP server address pool • option – Removes the DHCP server option • ping – Specifies default ping parameters used by a DHCP Server

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#no bootp ignore
rfs7000-37FABE(config-dhcp-policy-test)#

rfs7000-37FABE(config-dhcp-policy-test)#no option test1
rfs7000-37FABE(config-dhcp-policy-test)#
```

13.1.8 ping

dhcp-server-policy

Specifies ping parameters used by a DHCP Server

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ping timeout <1-10>
```

Parameters

timeout <1-10>	Select a value between 1 and 10 to specify the ping timeout (in seconds)

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#ping timeout 2
rfs7000-37FABE(config-dhcp-policy-test)#
```

13.1.9 dhcp-class

dhcp-server-policy

Configures DHCP Server class

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dhcp-class <DHCP-CLASS>
```

Parameters

<DHCP-CLASS>	Specify a DHCP class name

Example

```
rfs7000-37FABE(config-dhcp-policy-test)#dhcp-class dhcpclass1
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#?
DHCP class Mode commands:
  multiple-user-class  Enable multiple user class option
  no                   Negate a command or set its defaults
  option               Configure DHCP Server options

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal
```

13.1.10 dhcp-class-mode

Use the (config-dhcpclass) instance to configure DHCP user classes. The controller supports a maximum of 8 user classes per DHCP class. To navigate to this instance use the command:

```
rfs7000-37FABE(config-dhcp-policy-test)#dhcp-class dhcpclass1
rfs7000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#?
```

Table 13.4 Summarizes dhcp-class commands

Table 13.4 *dhcp-class Commands*

Command	Description	Reference
multiple-user-class	Enables multiple user class option	*page 13-43*
no	Negates a command or sets its default value	*page 13-44*
option	Configures DHCP server options	*page 13-45*

13.1.10.1 multiple-user-class

dhcp-class-mode

Enables multiple user class option

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
multiple-user-class
```

Parameters

None

Example

```
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#multiple-user-class
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#
```

13.1.10.2 no

dhcp-class-mode

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP7131
- AP650
- AP6511
- AP6532

Syntax

```
no [multiple-user-class|option]
```

Parameters

[multiple-user-class|option]	• multiple-user-class – Disables the multiple user class option • option – Unconfigures (removed updates for) DHCP server options

Example

```
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#no multiple-user-
class
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#
```

13.1.10.3 option

dhcp-class-mode

Configures DHCP server options

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
option user-class <WORD>
```

Parameters

user-class [<WORD>	• user-class – Configures DHCP server user-class options • <WORD> – Sets the ASCII value of user-class option to configure

Example

```
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#option user-class hex
rfs7000-37FABE(config-dhcp-policy-test-class-class1)#
```

CHAPTER 14 FIREWALL-POLICY

This chapter summarizes the firewall-policy commands within the CLI structure.

Use (config) instance to configure firewall-policy related configuration commands. To navigate to the config-fw-policy instance, use the following commands.

```
rfs7000-37FABE(config)#firewall-policy <policy-name>
rfs7000-37FABE(config)#firewall-policy test
rfs7000-37FABE(config-fw-policy-test)#?
Firewall policy Mode commands:
  alg                           Enable ALG
  clamp                         Clamp value
  dhcp-offer-convert            Enable conversion of broadcast dhcp offers to
                                unicast
  dns-snoop                     DNS Snooping
  firewall                      Wireless firewall
  flow                          Firewall flow
  ip                            Internet Protocol (IP)
  ip-mac                        Action based on ip-mac table
  logging                       Firewall enhanced logging
  no                            Negate a command or set its defaults
  proxy-arp                     Enable generation of ARP responses on behalf
                                of another device
  stateful-packet-inspection-l2 Enable stateful packet inspection in layer2
                                firewall
  storm-control                 Storm-control
  virtual-defragmentation       Enable virtual defragmentation for IPv4
                                packets (recommended for proper functioning
                                of firewall)

  clrscr                        Clears the display screen
  commit                        Commit all changes made in this session
  do                            Run commands from Exec mode
  end                           End current mode and change to EXEC mode
  exit                          End current mode and down to previous mode
  help                          Description of the interactive help system
  revert                        Revert changes
  service                       Service Commands
  show                          Show running system information
  write                         Write running configuration to memory or
                                terminal

rfs7000-37FABE(config-fw-policy-test)#
```

14.1 firewall-policy

Table 14.1 Summarizes default firewall policy commands

Table 14.1 *Firewall-policy Commands*

Command	Description	Reference
alg	Enables an algorithm	*page 14-3*
clamp	Sets a clamp value to limit TCP MSS to inner path-MTU for tunnelled packets	*page 14-4*
dhcp-offer-convert	Enables the conversion of broadcast DHCP offers to unicast	*page 14-5*
dns-snoop	Sets the timeout value for DNS entries	*page 14-6*
firewall	Configures the wireless firewall	*page 14-7*
flow	Defines a session flow timeout	*page 14-8*
ip	Configures IP for a selected component	*page 14-10*
ip-mac	Defines an action based on IP-MAC table	*page 14-14*
logging	Enables enhanced firewall logging	*page 14-15*
no	Negates a command or sets its default value	*page 14-16*
proxy-arp	Enables the generation of ARP responses on behalf of another device	*page 14-17*
stateful-packet-inspection-12	Enables stateful-packets-inspection in layer2 firewall	*page 14-18*
storm-control	Defines storm-control and sets logging	*page 14-19*
virtual-defragmentation	Enables virtual defragmentation for IPv4 packets	*page 14-21*

14.1.1 alg

firewall-policy

Enables a selected algorithm

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
alg [dns|ftp|sip|tftp]
```

Parameters

[dns|ftp|h323|http|sccp|sip|tftp]	Enables selected algorithm from the list • dns – Enables DNS ALG • ftp – Enables FTP ALG • sip – Enables SIP ALG • tftp – Enables TFTP ALG

Example

```
rfs7000-37FABE(config-fw-policy-default)# alg tftp
rfs7000-37FABE(config-fw-policy-default)#
```

14.1.2 clamp

firewall-policy

Sets the clamp value used to limit TCP MSS to inner path-MTU for tunnelled packets

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
clamp tcp-mss
```

Parameters

tcp-mss	Sets the clamp value used to limit TCP MSS to inner path-MTU for tunnelled packets

Example

```
rfs7000-37FABE(config-fw-policy-test)#clamp tcp-mss
rfs7000-37FABE(config-fw-policy-test)#
```

14.1.3 dhcp-offer-convert

firewall-policy

Enables the conversion of broadcast DHCP offers to unicast

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dhcp-offer-convert
```

Parameters

None

Example

```
rfs7000-37FABE(config-fw-policy-default)#dhcp-offer-convert
rfs7000-37FABE(config-fw-policy-default)#
```

14.1.4 dns-snoop

firewall-policy

Sets the timeout value for DNS entries

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dns-snoop entry-timeout <30-86400>
```

Parameters

entry-timeout <30-86400>	Sets the timeout value for DNS entries between 30 and 86400 seconds

Example

```
rfs7000-37FABE(config-fw-policy-test)#dns-snoop entry-timeout 35
rfs7000-37FABE(config-fw-policy-test)#
```

14.1.5 firewall

firewall-policy

Configures the wireless firewall

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
firewall enable
```

Parameters

firewall enable	Enables the wireless firewall

Example

```
rfs7000-37FABE(config-fw-policy-default)#firewall enable
rfs7000-37FABE(config-fw-policy-default)#
```

14.1.6 flow

firewall-policy

Defines the session flow timeout for different packet types

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
flow [dhcp|timeout]
flow dhcp stateful
flow timeout [icmp|other|tcp|udp]
flow timeout [icmp|other|udp] <1-32400>
flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset|
stateless-general] <1-32400>
flow timeout tcp established <15-32400>
```

Parameters

[dhcp|timeout]	Defines session flow timeout • dhcp stateful – Sets the DHCP flow between 1 and 32400 seconds • timeout [icmp|other|udp] <1-32400> – Sets the flow timeout based on the packet type • icmp – Sets the timeout for ICMP packets between 1 and 32400 • other – Sets the timeout for any packet type between 1 and 32400 seconds • udp <1-32400 – Sets the timeout for UDP packets between 1 and 32400 seconds • <1-32400> – Based on the packet type, the timeout is set between 1 and 32400 seconds • tcp[close-wait|established|reset|setup|stateless-fin-or-reset |stateless-general] – Based on the TCP state, the timeout is set between 1 and 32400 seconds • close-wait <1-32400> – Closed TCP flow • established <15-32400> – Established TCP flow. Set the timeout between 15 and 32400 seconds • reset <1-32400> – Reset TCP flow • setup <1-32400> – Opening TCP flow • stateless-fin-or-reset <1-32400> – Stateless TCP flow created with FIN or RESET packet • stateless-general <1-32400> – Stateless TCP Flow • <1-32400> – Based on the packet type, the timeout is set between 1 and 32400 seconds

Example

```
rfs7000-37FABE(config-fw-policy-default)#flow timeout icmp 4
rfs7000-37FABE(config-fw-policy-default)#

rfs7000-37FABE(config-fw-policy-default)#flow timeout tcp setup 8
rfs7000-37FABE(config-fw-policy-default)#

rfs7000-37FABE(config-fw-policy-default)#flow icmp stateful
rfs7000-37FABE(config-fw-policy-default)#
```

14.1.7 ip

firewall-policy

Configures a selected *Internet Protocol* (IP) component

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip [dos|tcp]
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|
ftp-bounce|invalid-protocol|ip-ttl-zero|ipspoof|land|option-route|
router-solicit|router-advt|smurf|snork|tcp-bad-sequence|tcp-fin-scan|
tcp-intercept|tcp-max-incomplete|tcp-null-scan | tcp-post-syn |
tcp-xmas-scan |tcphdrfrag |twinge|udp-short-hdr} [drop-only|
log-and-drop|log-only]

ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|
ftp-bounce|invalid-protocol|ip-ttl-zero|ipspoof|land|option-route|
router-solicit|router-advt|smurf|snork|tcp-bad-sequence|tcp-fin-scan|
tcp-intercept|| tcp-null-scan | tcp-post-syn |
tcp-xmas-scan |tcphdrfrag |twinge|udp-short-hdr|winnuke} [log-and-drop|
log-only] log-level [<0-8>|alerts|critical|debugging|emergencies|error|
informational|none|notifications|warnings]
ip dos {tcp-max-incomplete [high|low] <1-1000>}

ip tcp [adjust-mss <472-1460>|optimize-unnecessary-resends|
recreate-flow-on-out-of-state-syn|validate-icmp-unreachable|
validate-rst-ack-number|validate-rst-seq-number]
```

Parameters

dos {ascend| bcast-mcast-icmp |chargen|fraggle| ftp-bounce|invalid-protocol| ip-ttl-zero|ipspoof|land| option-route| router-solicit|router-advt| smurf|snork|tcp-bad-sequence|tcp-fin-scan| tcp-intercept|tcp-max-incomplete| tcp-null-scan| tcp-post-syn| tcp-xmas-scan |tcphdrfrag |twinge|udp-short-hdr} [drop-only|log-and-drop| log-only]log-level [<0-8>| alerts|critical|debugging| |emergencies| errors|informational|none|notifications| warnings]	Configures the *Denial of Service* (DOS) attack parameter • ascend – Enables ascend DoS checks • bcast-mcast-icmp – Detects broadcast/multicast ICMP traffic as an attack • chargen – Enables chargen DoS checks • fraggle – Enables fraggle DoS checks • ftp-bounce – Enables FTP bounce logs and sets the logging levels • invalid-protocol – Enables an invalid protocol DoS attack check and sets the logging levels for this attack • ip-ttl-zero – Enables a TCP IP TTL ZERO DoS attack check • ipspoof – Enables an IPSPOOF DoS attack check • land – Enables a LAND DoS attack check • option-route – Enables IP option route check • router-advt – Enables an ICMP router advertisement check • router-solicit – Enables an ICMP router solicit check • smurf log – Enables a smurf attack check • snork – Enables a packet check • tcp-intercept – Enables a TCP intercept • tcp-bad-sequence – Enables a TCP BAD SEQUENCE DoS attack check • tcp-fin-scan – Enables a TCP FIN SCAN DoS attack check
	• tcp-null-scan – Enables a TCP NULL SCAN DoS attack check • tcp-post-syn – Enables a TCP Post Syn DoS attack check • tcp-xmas-scan – Enables a TCP XMAS SCAN DoS attack check • tcphdrfrag – Enables a TCP Header Fragmentation attach check • twinge – Enables a twinge check • udp-short-hdr – Enables a UDP short header DoS attack check • winnuke – Enables WINNUKE DoS attack For all the above, the following parameters are common: • drop-only – Drops the packet only • log-and-drop log-level – Logs the details and drops the packet • log-only log-level – Logs the details only • log-level [<0-8>|alerts|critical|debugging| |emergencies|errors| informational|none|notifications|warnings] – Configures the log level for a DoS check

	For all the above DoS attacks, the following log-levels can be set • alerts – Immediate action needed (level 1) • critical – Critical conditions (level 2) • <0-8> – Select one numerical log level. All messages with and below this severity are logged • emergencies – System is unusable (level 0) • errors – Error conditions (level 3) • warnings – Warning conditions (level 4 • notifications – Normal but significant conditions (level 5) • informational – Informational messages (level 6) • debugging – Debugging messages (level 7) • none –Disable logging (level 8) • tcp -max-incomplete – Configures the maximum half-open TCP connections in the system • high <1-1000> – Sets the upper threshold value between 1 and 1000 • low <1-1000> – Sets the lower threshold value between 1 and1000
tcp [adjust-mss <472-1460> | optimize-unnecessary-resends |recreate-flow-on-out-of-state-syn| validate-icmp-unreachable | validate-rst-ack-number | validate-rst-seq-number]	Configures TCP protocol settings • adjust-mss <472-1460> – Sets TCP MSS adjustment value • <472-1460> – Sets the maximum value of TCP MSS option <472-1460> • optimize-unnecessary-resends – Enables checking of unnecessary resend of TCP packets • recreate-flow-on-out-of-state-syn – Allows a SYN packet to delete an old flow in TCP_FIN_FIN_STATE and TCP_CLOSED_STATE states and create a new flow • validate-icmp-unreachable – Enables checking of sequence number in ICMP unreachable error packets which aborts an established TCP flow • validate-rst-ack-number – Enables checking of acknowledgement number in RST packets which aborts a TCP flow in SYN (sent) state • validate-rst-seq-number – Enables checking of sequence number in RST packets which aborts an established TCP flow

Example

```
rfs7000-37FABE(config-fw-policy-default)#ip dos tcp-max-incomplete high 8
rfs7000-37FABE(config-fw-policy-default)#

rfs7000-37FABE(config-fw-policy-default)# ip dos land log-only log-level warnings
rfs7000-37FABE(config-fw-policy-default)#
```

```
rfs7000-37FABE(config-fw-policy-test)#ip tcp adjust-mss 475
rfs7000-37FABE(config-fw-policy-test)#
```

```
rfs7000-37FABE(config-fw-policy-test)#ip tcp recreate-flow-on-out-of-state-syn
rfs7000-37FABE(config-fw-policy-test)#

rfs7000-37FABE(config-fw-policy-test)#ip tcp validate-rst-seq-number
rfs7000-37FABE(config-fw-policy-test)#
```

14.1.8 ip-mac

firewall-policy

Defines an action based on the IP MAC table

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ip-mac [conflict|routing]
ip-mac conflict [drop-only|log-and-drop|log-only]
ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|
alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
ip-mac routing conflict [drop-only|log-and-drop|log-only]
ip-mac routing conflict [log-and-drop|log-only] log-level [<0-7>|
alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
```

Parameters

[conflict|routing]	• conflict – Enables IP Address v. MAC Address conflict detection • routing – Defines action based on routing table The following are common for the above: • drop-only – Drops the packets • log-and-drop – Logs and drop the packets • log-only – Logs the packets only • log-level – Configures the log level for DoS Checks • <0-7> – Logging severity level • alerts – Immediate action needed (severity=1) • critical – Critical conditions (severity=2) • debugging – Debugging messages (severity=7) • emergencies – System is unusable (severity=0) • errors – Error conditions (severity=3) • informational – Informational messages (severity=6) • notifications – Normal but significant conditions (severity=5) • warnings – Warning conditions (severity=4)

Example

```
rfs7000-37FABE(config-fw-policy-default)#ip-mac conflict-detection log
rfs7000-37FABE(config-fw-policy-default)#
```

14.1.9 logging

firewall-policy

Enables firewall enhanced logging

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
logging [icmp-packet-drop|malformed-packet-drop|verbose]
logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]
```

Parameters

[icmp-packet-drop| rawip-packet-drop] [all|rate-limited]	• icmp-packet-drop – Logs dropped ICMP packets failing sanity checks • malformed-packet-drop – Logs dropped IP packets failing sanity checks The following parameters are common for the above: • all – Logs all message instances • rate-limited – Enables rate-limiting. The granularity of rate -limiting is 20 seconds • verbose – Enables verbose logging (applicable to selected platforms only)

Example

```
rfs7000-37FABE(config-fw-policy-default)#logging rawip-packet-drop all
rfs7000-37FABE(config-fw-policy-default)#

rfs7000-37FABE(config-fw-policy-test)#logging malformed-packet-drop rate-limited
rfs7000-37FABE(config-fw-policy-test)#

rfs7000-37FABE(config-fw-policy-test)#logging verbose
rfs7000-37FABE(config-fw-policy-test)#
```

14.1.10 no

firewall-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [alg|clamp|dhcp-offer-convert|dns-snooping|firewall|flow|ip|
ip-mac|logging|proxy-arp|stateful-packet-inspection-l2 |storm-control|tcp|
virtual-defragmentation]
```

Parameters

alg	Disables alg
clamp	Deletes a clamp value
dhcp-offer-convert	Disables conversion broadcast DHCP offers to unicast
dns-snoop	Disables DNS snooping
firewall	Unconfigures the wireless firewall
flow	Defines a session flow timeout
ip	Configures a selected *Internet Protocol* (IP) component
ip-mac	Defines an action based on the IP-MAC table
logging	Disables firewall enhanced logging
proxy-arp	Disables generation of ARP responses on behalf of another device
stateful-packet-inspection-l2	Disables stateful packet inspection in a layer2 firewall
storm-control	Defines storm-control logging configuration
tcp	Disables the TCP protocol
virtual-defragmentation	Disables virtual defragmentation

Example

```
rfs7000-37FABE(config-fw-policy-default)#no storm-control arp log
rfs7000-37FABE(config-fw-policy-default)#s

rfs7000-37FABE(config-fw-policy-default)#no dhcp-offer-convert
rfs7000-37FABE(config-fw-policy-default)#
```

14.1.11 proxy-arp

firewall-policy

Enables the generation of ARP responses on behalf of another device

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
proxy-arp
```

Parameters

None

Example

```
rfs7000-37FABE(config-fw-policy-default)#proxy-arp
rfs7000-37FABE(config-fw-policy-default)#
```

14.1.12 stateful-packet-inspection-12

firewall-policy

Enables a stateful packet inspection at the layer2 firewall

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
stateful-packet-inspection-l2
```

Parameters

None

Example

```
rfs7000-37FABE(config-fw-policy-test)#stateful-packet-inspection-l2
rfs7000-37FABE(config-fw-policy-test)#
```

14.1.13 storm-control

firewall-policy

Storm control limits the amount of multicast, unicast and broadcast frames accepted and forwarded by the device. Messages are logged based on their severity level.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
storm-control [arp|broadcast|multicast|unicast] [level|log]
storm-control [arp|bcast|mcast|ucast] level <1-1000000> [fe|ge|
port-channel|up1|wlan]
storm-control [arp|bcast|mcast|ucast] level <1-1000000> [fe <1-4>|ge <1-8>|
port-channel <1-8>|up1|wlan <WLAN>]
storm-control [arp|bcast|mcast|ucast] log [<0-7>|alert|critical|
debugging|emergencies|errors|informational|none|notifications
|warnings]
```

Parameters

[arp|bcast|mcast|ucast]{log} [<0-7>|alert|critical |debugging| emergencies|errors| informational| none|notifications |warnings]	• arp – The traffic type is ARP • bcast – The traffic type is broadcast • mcast – The traffic type is multicast • ucast – The traffic type is unicast For all the above, the following level and log options can be set • level <1-1000000> [ge <1-8>|port-channel <1-8>| up1|wlan <WLAN>] – Performs packet rate limiting • <1-1000000> – Specify the allowed rate in packets/sec from <1-1000000> • ge <1-8> – Select a physical port to apply from 1-8 • port-channel <1-8> – Select a port-channel from 1-8 • up1 – Applies on the Uplink interface • wlan <WLAN> – Select a WLAN to apply. The existing WLAN must be specified • log – Enables logging • <0-8> – Select one numerical log level. All messages with and below this severity are logged • emergencies – System is unusable (level 0) • alerts – Immediate action needed (level 1) • critical – Critical conditions (level 2 • errors – Error conditions (level 3) • warnings – Warning conditions (level 4) • notifications – Normal but significant conditions exist (level 5) • informational – Informational messages (level 6 • debugging – Debugging messages (level 7)

Example

```
rfs7000-37FABE(config-fw-policy-default)# storm-control unicast level 2 ge 2
rfs7000-37FABE(config-fw-policy-default)#

rfs7000-37FABE(config-fw-policy-default)#storm-control bcast log notifications
rfs7000-37FABE(config-fw-policy-default)#
```

14.1.14 virtual-defragmentation

firewall-policy

Enables the virtual defragmentation for IPv4 packets

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
virtual-defragmentation {maximum-defragmentation-per-host <1-16384>| maximum-
fragments-per-datagram <2-8129>|minimum-first-fragment-length
<8-1500>}
```

Parameters

maximum-defragmentation-per-host <1-16384>	Defines the maximum active IPv4 defragmentation per host. Sets a value between 1 and 16384
maximum-fragments-per-datagram <2-8129>	Defines the maximum IPv4 fragments per datagram. Sets a value between 2 and 8129
minimum-first-fragment-length <8-1500>	Defines the minimum length required for the first IPv4 fragment. Sets a value between 8 and 1500

Example

```
rfs7000-37FABE(config-fw-policy-test)#virtual-defragmentation maximum-fragments-per-
datagram 10
rfs7000-37FABE(config-fw-policy-test)#

rfs7000-37FABE(config-fw-policy-test)#virtual-defragmentation minimum-first-
fragment-length 100
rfs7000-37FABE(config-fw-policy-test)#
```

CHAPTER 15 IGMP-SNOOP-POLICY

This chapter summarizes igmp-snoop-policy commands within the CLI structure.

Use the (config) instance to configure igmp-snoop-policy related configuration commands. To navigate to the config-igmp-snoop-policy instance, use the following commands:

```
rfs7000-37FABE(config)#igmp-snoop-policy <policy-name>
rfs7000-37FABE(config)#igmp-snoop-policy test

rfs7000-37FABE(config-igmp-snoop-policy-test)#?
  igmp-snooping           Enable IGMP snooping
  no                      Negate a command or set its defaults
  querier                 Configure IGMP querier
  robustness-variable     Configure IGMP Robustness Variable
  unknown-multicast-fwd   Forward Unknown Multicast Packet

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs7000-37FABE(config-igmp-snoop-policy-test)#
```

15.1 igmp-snoop-policy

Table 15.1 Summarizes igmp-snoop-policy commands

Table 15.1 *igmp-snooping Commands*

Command	Description	Reference
igmp-snooping	Enables IGMP snooping	*page 15-3*
querier	Configures IGMP querier	*page 15-4*
robustness-variable	Configures IGMP Robustness variable	*page 15-5*
unknown-multicast-fwd	Forwards unknown multicast packets	*page 15-6*
no	Negates a command or sets its default value	*page 15-7*

15.1.1 igmp-snooping

igmp-snoop-policy

Enables IGMP snooping

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
igmp-snooping
```

Parameters

None

Example

```
rfs7000-37FABE(config-igmp-snoop-policy-test)#igmp-snooping
rfs7000-37FABE(config-igmp-snoop-policy-test)#
```

15.1.2 querier

igmp-snoop-policy

Configures the IGMP querier

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
querier query-interval <1-18000>
```

Parameters

query-interval <1-18000>	• querier query-interval <1-18000> – Configures the IGMP querier value from the selected interval • <1-18000> – Select an interval between 1 and 18000

Example

```
rfs7000-37FABE(config-igmp-snoop-policy-test)#querier query-interval 10
rfs7000-37FABE(config-igmp-snoop-policy-test)#
```

15.1.3 robustness-variable

igmp-snoop-policy

Configures an IGMP robustness variable

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
robustness-variable <1-7>
```

Parameters

<1-7>	Select a value between 1 and 7 to configure IGMP robustness

Example

```
rfs7000-37FABE(config-igmp-snoop-policy-test)#robustness-variable 1
rfs7000-37FABE(config-igmp-snoop-policy-test)#
```

15.1.4 unknown-multicast-fwd

igmp-snoop-policy

Forwards unknown multicast packets

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
unknown-multicast-fwd
```

Parameters

None

Example

```
rfs7000-37FABE(config-igmp-snoop-policy-test)#unknown-multicast-fwd
rfs7000-37FABE(config-igmp-snoop-policy-test)#
```

15.1.5 no

igmp-snoop-policy

Negates a command or sets its default vale

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no  [igmp-snooping|querier|robustness-variable|unknown-multicast-fwd]
```

Parameters

no [igmp-snooping|querier |robustness-variable| unknown-multicast-fwd]	• igmp-snooping – Disables IGMP snooping • querier – Unconfigures the IGMP querier • robustness-variable – Reverts to the default IGMP robustness variable • unknown-multicast-fwd – Does not forward unknown multicast packets

Example

```
rfs7000-37FABE(config-igmp-snoop-policy-test)#no igmp-snooping
rfs7000-37FABE(config-igmp-snoop-policy-test)#
```

NOTE: write, clrscr, do, exit, help, commit, revert, show, and service are common commands. For more information, see *Chapter 5, COMMON COMMANDS*.

CHAPTER 16 MINT-POLICY

This chapter summarizes mint-policy commands within the CLI structure.

All communication using the MiNT transport layer can be optionally secured. This includes confidentiality, integrity and authentication of all communications. In addition, a device can be configured to communicate over MiNT with other devices authorized by an administrator.

Use the (config) instance to configure mint-policy related configuration commands. To navigate to the mint-policy instance, use the following commands:

```
rfs7000-37FABE(config)#mint-policy global-default
rfs7000-37FABE(config-mint-policy-global-default)#

rfs7000-37FABE(config-mint-policy-global-default)#?

Mint Policy Mode commands:
  level                Mint routing level
  mtu                  Configure the global Mint MTU
  no                   Negate a command or set its defaults
                         requests from unknown devices
  udp                  Configure mint UDP/IP encapsulation

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information

  write                Write running configuration to memory or terminal
```

16.1 mint-policy

Table 16.1 Summarizes mint-policy commands

Table 16.1 *mint-policy Commands*

Command	Description	Reference
level	Configures the MiNT routing level	*page 16-3*
mtu	Configures the global MiNT MTU	
no	Negates a command or sets its default value	*page 16-9*
udp	Configures MiNT UDP/IP encapsulation parameters	*page 16-8*

16.1.1 level

mint-policy

Configures the MiNT routing level

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
level 2 area-id <1-4294967295>
```

Parameters

2 area-id <1-4294967295>	Configures level2 inter-site value • area-id <1-4294967295> – Configures routing area identifier value between <1-4294967295>

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#level 2 area-id 2
rfs7000-37FABE(config-mint-policy-global-default)#

rfs7000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 level 2 area-id 2
rfs7000-37FABE(config-mint-policy-global-default)#
```

16.1.2 mtu

mint-policy

Configures the global MiNT MTU

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mtu <900-1500>
```

Parameters

<900-1500>	Specifies the maximum packet size. Will be rounded down to nearest (4 + a multiple of 8).

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#mtu 1000
rfs7000-37FABE(config-mint-policy-global-default)#
```

16.1.3 re-join timeout

mint-policy

Specifies the timeout after which the device attempts to join a new security domain

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
re-join timeout <30-4294967295>
```

Parameters

<30-4294967295>	When unable to adopt, a device attempts to join a new security domain. Specify the timeout in seconds between 30 and 4294967295.

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#rejoin-timeout 35
rfs7000-37FABE(config-mint-policy-global-default)#
```

16.1.4 security-level

mint-policy

Configures the MiNT security level used by all devices

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
secuirty-level [control|control-and-data|none]
```

Parameters

[control| control-and-data|none]	• control – Configures MiNT security for control packets • control-and-data – Configures MiNT security for control and data packets • none – No MiNT security

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#security-level control-and-data
rfs7000-37FABE(config-mint-policy-global-default)#
```

16.1.5 sign-unknown-device

mint-policy

Accepts, sign and certificate signing requests from unknown devices automatically

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
sign-unknown-device
```

Parameters

None

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#sign-unknown-device
rfs7000-37FABE(config-mint-policy-global-default)#
```

16.1.6 udp

mint-policy

Configures MiNT UDP/IP encapsulation parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
udp port <2-65534>
```

Parameters

port <2-65534>	Configures the default UDP port used for MiNT control packet encapsulation between <2-65534>.

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#udp port 1024
rfs7000-37FABE(config-mint-policy-global-default)#
```

16.1.7 no

mint-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [level|mtu|udp|rejoin-timeout|security-level|sign-unknown-device]
```

Parameters

no [level|mtu|udp| rejoin-timeout| security-level| sign-unknown-device]	• rejoin-timeout – Resets the rejoin timeout to its default • security-level – Resets the MiNT security level to its default • sign-unknown-device – Disables automatic certificate signing • level – Resets MiNT routing level • mtu – Uses default global MiNT MTU • udp – Resets MiNT UDP/IP encapsulation to default configuration

Example

```
rfs7000-37FABE(config-mint-policy-global-default)#no sign-unknown-device
rfs7000-37FABE(config-mint-policy-global-default)#
```

NOTE: The commands clrscr, commit, exit, end, help, write, revert, service and show are common commands. For more information, see *Chapter 5, COMMON COMMANDS*.

CHAPTER 17 MANAGEMENT-POLICY

This chapter summarizes management-policy commands within the CLI structure.

Use the (config) instance to configure management-policy related configuration commands. To navigate to the management-policy instance, use the following commands:

```
rfs7000-37FABE(config)#management-policy  <policy-name>
rfs7000-37FABE(config)#management-policy default
```

To commit a management-policy, at least one admin user account must always be present in the management-policy:

```
rfs7000-37FABE(config-management-policy-default)#user superuser password 1 symbol123
rfs7000-37FABE(config-management-policy-default)#commit
rfs7000-37FABE(config-management-policy-default)#
```

rfs7000-37FABE(config-management-policy-default)#?

```
Management Mode commands:
  aaa-login             Set authentication for logins
  banner                Define a login banner
  ftp                   Enable FTP server
  http                  Hyper Text Terminal Protocol (HTTP)
  https                 Secure HTTP
  idle-session-timeout  Configure idle timeout for a configuration session (UI
                        or mapsh)
  no                    Negate a command or set its defaults
  restrict-access       Restrict management access to the device
  snmp-server           SNMP
  ssh                   Enable ssh
  telnet                Enable telnet
  user                  Add a user account

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs7000-37FABE(config-management-policy-default)#
```

17.1 management-policy

Table 17.1 Summarizes management-policy commands

Table 17.1 *management-policy Commands*

Command	Description	Reference
aaa-login	Sets authentication for logins	*page 17-3*
banner	Defines a login banner name	*page 17-5*
ftp	Enables a FTP server	*page 17-6*
http	Enables a HTTP server	*page 17-8*
https	Enables a secure HTTPs server	*page 17-9*
idle-session-timeout	Sets the duration after which a configuration session is timed out	*page 17-10*
no	Negates a command or sets its default value	*page 17-11*
restrict-access	Restricts management access to a set of hosts or subnets	*page 17-12*
snmp-server	Sets the SNMP-server configuration	*page 17-13*
ssh	Enables SSB	*page 17-16*
telnet	Enables Telnet	*page 17-17*
user	Creates a new user account	*page 17-18*

17.1.1 aaa-login

management-policy

Configures the current authentication, authorization and accounting (aaa) login settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
aaa-login [local|radius]
aaa-login radius [external|fallback|server]
aaa-login radius server host <A.B.C.D> secret [0|2] <WORD> {attempts
<1-10>|time-out <1-60>|udp-port  <0-65536>}
```

Parameters

local	Sets local authentication

radius [external|fallback| server]]	Configures an external RADIUS server
	• external – Requires external RADIUS authentication
	• fallback – Attempts external RADIUS authentication, uses local authentication when failed
	• server host <A.B.C.D> secret [0|2] <WORD> {attempts <1-10> |time-out <1-60> | udp-port <0-65536>} – Defines an external RADIUS server
	  • host – Sets the IP address of RADIUS server to configure
	  • <A.B.C.D> – Specify the IP address of RADIUS server to configure
	  • secret [0|2] <WORD> – Enter a clear text secret
	  • 0 – Password is encrypted with secret
	  • 2 – Password is UNENCRYPTED
	  • <WORD> – Enter text of shared secret, up to 127 characters
	  • attempts <1-10> – Specifies the number of attempts to connect to RADIUS server
	  • timeout <1-60> – Specify the timeout value between 1and 60 seconds for the server's response
	  • udp-port <0-65536> – Specify the UDP port number for the RADIUS server. The default port is 1812

Usage Guidelines

Use an AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server

Example

```
rfs7000-37FABE(config-management-policy-default)#aaa-login radius radius-server host
172.16.10.9 udp-port 3
rfs7000-37FABE(config-management-policy-default)#
```

```
rfs7000-37FABE(config-management-policy-default)#aaa-login local
rfs7000-37FABE(config-management-policy-default)#
```

17.1.2 banner

management-policy

Defines ~~a~~the login banner message of the day. Use this command to display messages to a user as soon as login happens.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
banner motd <LINE>
```

Parameters

motd <LINE>	Sets the message of the day banner

Example

```
rfs7000-37FABE(config-management-policy-default)#banner motd GoodDay
rfs7000-37FABE(config-management-policy-default)#
```

17.1.3 ftp

management-policy

Configures FTP server parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ftp {password [1 <WORD>|<WORD>]|rootdir <DIR>|username}
ftp username <WORD> password [1 <WORD> rootdir <DIR>|<WORD> rootdir <DIR>]
```

Parameters

password [1 <WORD>|<WORD>]	Configures ftp password • 1 <WORD> – Enter the encrypted password (Eg: if copy-pasting from another device) • < WORD> – Enter the password
rootdir <DIR>	Configures a FTP root directory
username <WORD> password [1 <WORD> rootdir <DIR>|<WORD> rootdir <DIR>]	Defines a FTP username • password – Configures the FTP password • 1 <WORD> rootdir <DIR> – Enter the encrypted password (Eg: if copy-pasting from another device) • rootdir <DIR> – Sets the ROOT directory location of the FTP server • <DIR> – The root directory for the FTP server • <WORD> – Enter the password to configure

Usage Guidelines

The string size of encrypted password (option 1, Password is encrypted with SHA1 algorithm) must be exactly 40 characters

Example

```
rfs7000-37FABE(config-management-policy-test)#ftp password word
rfs7000-37FABE(config-management-policy-test)#

rfs7000-37FABE(config-management-policy-test)#ftp password 1 root
rfs7000-37FABE(config-management-policy-test)#

rfs7000-37FABE(config-management-policy-test)#ftp rootdir dir
rfs7000-37FABE(config-management-policy-test)#

rfs7000-37FABE(config-management-policy-test)#ftp username superuser password 1 word
rootdir dir
rfs7000-37FABE(config-management-policy-test)#
```

```
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 ftp username root password 1 word rootdir dir
 no ssh
 user superuser password 1
4e03aaf1065294ba86d19da984347e38dfbaa9955335dc354748cb4f9a16e0a9
rfs7000-37FABE(config-management-policy-test)#
```

17.1.4 http

management-policy

Defines HTTP server settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
http <server>
```

Parameters

server	Enables the HTTP server

Example

```
rfs7000-37FABE(config-management-policy-test)#http server
rfs7000-37FABE(config-management-policy-test)#
```

17.1.5 https

management-policy

Configures secure HTTPs server parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
https server
```

Parameters

server	Enables the HTTPS server

Example

```
rfs7000-37FABE(config-management-policy-test)#https server trustpoint testtrust
rfs7000-37FABE(config-management-policy-test)#
```

17.1.6 idle-session-timeout

management-policy

Configures a configuration session's idle timeout duration. After the session has been idle for this time duration, the session is automatically timed out.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
idle-session-timeout <TIME>
```

Parameters

<TIME>	The time duration in minutes after which a configuration session is timed out. Enter a value in the range of 0 and 1440 where zero (0) indicates that the configuration session is never timed out.

17.1.7 no

management-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [banner|exec-timeout|ftp|http|https|secure-management|
snmp-server|ssh|telnet|user]
```

Parameters

[banner|exec-timeout| ftp|http|https| secure-management| snmp-server| ssh|telnet|user]	• banner – Defines a login banner • exec-timeout – Disables the session timeout • ftp – Enables a FTP server • http – Enables the hypertext terminal protocol (HTTP) • https – Enables secure HTTP • secure-management – Disables secure management • snmp-server – Disables SNMP • ssh – Disables SSH • telnet – Disables Telnet • user – Removes user account

Example

```
rfs7000-37FABE(config-management-policy-test)#no  ssh port
rfs7000-37FABE(config-management-policy-test)#

rfs7000-37FABE(config-management-policy-test)#no secure-management
rfs7000-37FABE(config-management-policy-test)#
```

17.1.8 restrict-access

management-policy

Restricts management access to a set of hosts or subnets

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
restrict-access [host|ip-access-list|subnet]
restrict-access host <A.B.C.D> {<A.B.C.D>|log [all|denied-only]|subnet <A.B.C.D/M>
{<A.B.C.D>/M|log [all|denied-only]}}
restrict-access ip-access-list <IP-ACCESS-LIST>
restrict-access subnet <A.B.C.D/M> {<A.B.C.D>/M|log [all|denied-only]|host <A.B.C.D>
{<A.B.C.D>|log [all|denied-only]}}
```

Parameters

[host|ip-access-list|subnet]	• host <A.B.C.D> {<A.B.C.D>|log [all|denied-only]|subnet <A.B.C.D/M> {<A.B.C.D>/M|log [all|denied-only]}} – Restricts management access to specific hosts
	• ip-access-list <IP-ACCESS-LIST> – Uses an IP access list to filter requests for management access
	  • <IP-ACCESS-LIST> – Specify the IP access list to be used
	• subnet<A.B.C.D/M> {<A.B.C.D>/M|log [all|denied-only]|host <A.B.C.D> {<A.B.C.D>|log [all|denied-only]}} – Restricts management access to specific subnets
	  • <A.B.C.D>/M – Specify a subnet IP to restrict management access
	The following parameters are common for all the above:
	  • log – Configures logging policy for management access
	  • all – Logs all the requests for management access (includes denied and permitted)
	  • denied-only – Logs denied requests for management access

Example

```
rfs7000-37FABE(config-management-policy-default)#restrict-access host 172.16.10.2
log all
rfs7000-37FABE(config-management-policy-default)#

rfs7000-37FABE(config-management-policy-default)#restrict-access subnet
172.16.10.20/24 host 1.2.3.4 log all
rfs7000-37FABE(config-management-policy-default)#

rfs7000-37FABE(config-management-policy-default)#restrict-access host 1.2.3.4 log
denied-only
rfs7000-37FABE(config-management-policy-default)#
```

17.1.9 snmp-server

management-policy

Configures SNMP engine parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
snmp-server [community|enable|host|manager|user]
snmp-server enable traps
snmp-server community <WORD> [ro|tw]
snmp-server host <A.B.C.D> [v2c|v3] {<1-65535>}
snmp-server manager [all|v2|v3]
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 [auth md5|encrypted [auth
md5|des auth md5][0|2|<WORD>]
```

Parameters

community <WORD> [ro|tw]	Sets the community string and access privileges.
	• <WORD> – Sets the community string
	  • ro – Assigns read-only access to this community string
	  • rw – Assigns read-write access to this community string

enable traps	Enables SNMP traps

host <A.B.C.D> [v2c|v3] {<1-65535>}	SNMP server host
	• <A.B.C.D> – Sets the SNMP server host IP address
	  • v2c – Use SNMP version 2c
	  • v3 – Use SNMP version 3
	  • <1-65535> – Select a value between 1 and 65535 to configure the port. The default port is 162

manager [all|v2|v3]	Enables SNMP manager • all – Enables SNMP version v2 and v3 • v2 – Enables SNMP version v2 • v3 – Enable SNMP version v3

snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 [auth md5|encrypted [auth md5|des auth md5][0|2|<WORD>]]	Defines a user who can access the SNMP engine
	• snmpmanager – Sets the user as a manager
	• snmpoperator – Sets the user as a operator
	• snmptrap – Sets the user as a SNMP trap user
	The following parameters are common for all the above types of users:
	• v3 [auth md5|encrypted] – Use the SNMPv3 as the security model
	  • auth md5 – Authentication protocol
	  • md5 – Uses the HMAC-MD5 algorithm for authentication
	  • encrypted [auth|des] – Encrypted protocol
	  • auth md5 – Sets authentication parameters for the user
	  • md5 [0|2|<WORD>] – Uses the HMAC-MD5 algorithm for authentication
	  • 0 – Enter a clear text password
	  • 2 – Enter an encrypted password
	  • <WORD> – Specify a password for authentication and privacy protocols
	  • des – Uses CBC-DES for privacy

Example

```
rfs7000-37FABE(config-management-policy-test)#snmp-server community snmp1 ro
rfs7000-37FABE(config-management-policy-test)#

rfs7000-37FABE(config-management-policy-test)#snmp-server host 172.16.10.23 v3 162
rfs7000-37FABE(config-management-policy-test)#commit
rfs7000-37FABE(config-management-policy-test)#

rfs7000-37FABE(config-management-policy-test)#snmp-server user snmpmanager v3 auth
md5 symbol123
rfs7000-37FABE(config-management-policy-test)#
rfs7000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 https server trustpoint testtrust
```

```
 ftp username root password 1 word rootdir dir
 no ssh
 user superuser password 1
4e03aaf1065294ba86d19da984347e38dfbaa9955335dc354748cb4f9a16e0a9
 snmp-server community snmp1 ro
 snmp-server enable traps
 snmp-server host 172.16.10.23 v3 162
 snmp-server host 172.16.10.3 v3 162
 snmp-server host 172.16.10.23 v2c 4
rfs7000-37FABE(config-management-policy-test)#
```

17.1.10 ssh

management-policy

Configures SSH parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`ssh {port} <1-65535>`

Parameters

port <1-65535>	Select a value between 1 and 165535 to configure a SSH port. The default port value is 22

Example

```
rfs7000-37FABE(config-management-policy-test)#ssh port 162 ?
rfs7000-37FABE(config-management-policy-test)#
```

17.1.11 telnet

management-policy

Enables Telnet settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

`telnet {port} <1-65535>`

Parameters

port <1-65535>	Select a Telnet port value between 1 and 165535. The default port is 23.

Example

```
rfs7000-37FABE(config-management-policy-test)#telnet port 23
rfs7000-37FABE(config-management-policy-test)#
```

17.1.12 user

management-policy

Creates a new user account

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
user <WORD> password [0|1|<WORD>]
user <WORD> password [0|1|<WORD>] role [helpdesk|monitor|
nework-admin|security-admin|superuser|system-admin|web-user-admin] access
[all|console|ssh|telnet]
user <WORD> password [0|1|<WORD>] role [helpdesk|monitor|
nework-admin|security-admin|superuser|system-admin|web-user-admin] access
{all|console|ssh|telnet}
```

Parameters

<WORD> password	• <WORD> – Specify a user account name to create an user account
	• password – Specify a user password
	  • 0 – Enter the clear text password
	  • 1 – Enter an encrypted password
	  • <WORD> – Enter the password to configure
	The following parameters are common for both encrypted password and generic password
	  • role [helpdesk|monitor|nework-admin|security-admin| superuser|system-admin|web-user-admin] access [all| console|ssh|telnet] – Configures a role for the new user, assign a role from the list:
	  • helpdesk – Helpdesk
	  • monitor – Monitor
	  • network-admin – Network administrator
	  • security-admin – Security administrator
	  • superuser – Superuser
	  • system-admin – System administrator
	  • web-user-admin – Web user administrator
	  • access – Configures user access
	  • all – Allow access to all the modes
	  • console – Allows console access
	  • ssh – Allows SSH access
	  • telnet – Allows Telnet access

Example

```
rfs7000-37FABE(config-management-policy-test)#user testuser password moto123
rfs7000-37FABE(config-management-policy-test)#commit
rfs7000-37FABE(config-management-policy-default)#user george password 1 symbol12 role
security-admin access console ssh telnet web
rfs7000-37FABE(config-management-policy-default)#
```

NOTE: The commands clrscr, commit, do, exit, help, write, revert, service and show are common commands. Refer to *Chapter 5, COMMON COMMANDS* for more information.

CHAPTER 18 RADIUS-POLICY

This chapter summarizes RADIUS-Group, RADIUS-Server and RADIUS-User-Policy commands in detail.

Use the (config) instance to configure RADIUS-Group related configuration commands. This command creates a group within the existing RADIUS group. To navigate to the radius-group instance, use the following commands:

```
rfs7000-37FABE(config)#radius-group <group-name>
rfs7000-37FABE(config)#radius-group test
rfs7000-37FABE(config-radius-group-test)#?
Radius user group configuration commands:
  guest       Make this group a Guest group
  no          Negate a command or set its defaults
  policy      Radius group access policy configuration
  rate-limit  Set rate limit for group

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs7000-37FABE(config-radius-group-test)#
```

18.1 radius-group

Sets RADIUS user group parameters

Table 18.1 Summarizes RADIUS group commands

Table 18.1 *radius-group Commands*

Command	Description	Reference
guest	Enables guest access for the newly created group	*page 18-3*
no	Negates a command or sets its default values	*page 18-8*
policy	Configures RADIUS group access policy parameters	*page 18-4*
rate-limit	Sets the default rate limit per user in kbps, and applies it to all enabled WLANs	*page 18-7*

18.1.1 guest

radius-group

Manages a guest user linked with a hotspot. Create a guest-user and associates it with the guest group. The guest user and policies are used for hotspot authentication/authorization.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
guest
```

Parameters

None

Example

```
rfs7000-37FABE(config-radius-group-test)#guestrfs7000-37FABE(config-radius-group-
test)#
```

18.1.2 policy

radius-group

Sets the authorization policies for a particular group day/time of access, WLANs etc.

NOTE: A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN (as defined within the WLAN Configuration screen).

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
policy [access|day|role|ssid|time|vlan <1-4094>]
policy access [all|console|ssh|telnet|web]
policy access [all|console|ssh|telnet|web] {all|console|ssh|telnet|web}
policy role [helpdesk|monitor|network-admin|security-admin|
super-user|system-admin|web-user-admin]
policy ssid <WORD>
policy day[all|fri|mo|sa|su|tu|we|th|weekdays]{all|fri|mo|sa|su|tu|
we|th|weekdays}
policy time start <HH:MM> end <HH:MM>
```

Parameters

access [all|console|ssh|telnet|web]	Sets management group access • all – Allows all access • console – Allows console access • ssh – Allows SSH access • telnet – Allows Telnet access • web – Allows Web access
day [all|fri|mo|sa|su|th|tu|we|week days]	Configures the access day for this group • all – All days (from Sunday to Saturday) • fri – Friday • mo – Monday • sa – Saturday • su – Sunday • th – Thursday • tu – Tuesday • we – Wednesday • weekdays – Configures the policy access in weekdays (Monday to Friday)
role [helpdesk|monitor| network-admin| security-admin| super-user| system-admin| web-user-admin]	Sets the management group role • helpdesk – Helpdesk • monitor – Monitor • network-admin – Network administrator • security-admin – Security administrator • superuser – Superuser • system-admin – System administrator • web-user-admin – Web user administrator
ssid <WORD>	Configures SSID for this group • <WORD> – Specify a case-sensitive alphanumeric SSID, up to 32 characters
time start<HH:MM> end <HH:MM>	Configures time of access for this group • start <HH:MM> – Enter the start time in the format: HH:MM for ex., 13:30 means user can login only after 1:30 PM • end<HH:MM> – Enter the end time in the format: HH:MM for ex., 17:30 means that until 5:30 PM, the user is allowed to remain logged in
vlan <1-4094>	Select a value between 1 and 4094 to configure a VLAN ID for this group

Example

```
rfs7000-37FABE(config-radius-group-test)#policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#

rfs7000-37FABE(config-radius-group-test)#policy wlan wlan1
rfs7000-37FABE(config-radius-group-test)#

rfs7000-37FABE(config-radius-group-test)#show context
radius-group test
 guest-group
 policy vlan 2
 policy wlan wlan1
 policy time start 13:30 end 17:30
rfs7000-37FABE(config-radius-group-test)#
```

18.1.3 rate-limit

radius-group

Sets the rate limit for the RADIUS server group

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rate-limit [from-air|to-air] <100-1000000>
```

Parameters

to-air <100-1000000>	Downlink direction from the network to the wireless client • <100-1000000> – Specifies the rate in the range of <100-1000000>
from-air <100-1000000>	Uplink direction from the wireless client to the network • <100-1000000> – Specifies the rate in the range of <100-1000000>

Usage Guidelines

Use `[no] rate-limit [wired-to-wireless|wireless-to-wired]` to remove the rate limit applied to the group.

`[no] rate-limit [wireless-to-wired]` sets the rate limit back to unlimited

Example

```
rfs7000-37FABE(config-radius-group-test)##rate-limit to-air 101
rfs7000-37FABE(config-radius-group-test)#
```

18.1.4 no

radius-group

Negates a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [guest|policy|rate-limit]
```

Parameters

guest|policy|rate-limit]	• guest – Makes this group a non-guest group • policy – Removes RADIUS group access policy configuration • rate-limit – Removes rate-limit for the RADIUS group

Example

```
rfs7000-37FABE(config-radius-group-test)#no guest
rfs7000-37FABE(config-radius-group-test)#
```

18.2 radius-server-policy

Creates an onboard device RADIUS policy

Use the (config) instance to configure RADIUS-Server-Policy related configuration commands. To navigate to the RADIUS-Server-Policy instance, use the following commands:

```
rfs7000-37FABE(config)#radius-server-policy <policy-name>
rfs7000-37FABE(config)#radius-server-policy test
rfs7000-37FABE(config-radius-server-policy-test)#
```

Table 18.2 Summarizes radius-server-policy commands

Table 18.2 *radius-server-policy Commands*

Commands	Description	Reference
authentication	Configures RADIUS authentication parameters	*page 18-10*
crl-check	Enables a certificate revocation list (CRL) check	*page 18-11*
ldap-group-verification	Enables LDAP group verification settings	*page 18-12*
ldap-server	Configures LDAP server parameters	*page 18-13*
local	Configures a local RADIUS realm	*page 18-15*
nas	Configures the key that must be sent to a RADIUS client	*page 18-16*
no	Negates a command or sets its defaults	*page 18-17*
proxy	Configures RADIUS proxy server settings	*page 18-18*
session-resumptionn	Enables session resumption	*page 18-19*
use	Defines settings used with the RADIUS server Policy	*page 18-20*

18.2.1 authentication

radius-server-policy

Configures RADIUS authentication parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
authentication [data-source|eap-auth-type]
authentication data-source [ldap|local]
authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|
ttls-mschapv2|ttls-pap]
```

Parameters

data-source [ldap|local]	Enables the RADIUS datasource for user authentication • ldap – Remote LDAP server • local – Local user database
eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]	Enables RADIUS EAP and default authentication type configuration • all – Enables both ttls and peap • peap-gtc – Eap type peap with default auth type gtc • peap-mschapv2 – EAP type peap with default auth type mschapv2 • tls – EAP type tls • ttls-md5 – EAP type ttls with default auth type md5 • ttls-mschapv2 – EAP type ttls with default auth type mschapv2 • ttls-pap – EAP type ttls with default auth type pap

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#authentication eap-auth-type tls
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.2 crl-check

radius-server-policy

Enables certificate revocation list (CRL) check

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
crl-check
```

Parameters

None

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#crl-check
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.3 ldap-group-verification

radius-server-policy

Enables LDAP group verification settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ldap-group-verification
```

Parameters

None

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#ldap-group-verification
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.4 ldap-server

radius-server-policy

Configures LDAP server parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ldap-server [dead-period <0-600>|primary|secondary]
ldap-server [primary|secondary] host <A.B.C.D> port <1-65535> login <WORD> bind-dn
<WORD> base-dn <WORD> passwd [0|2|<WORD>] passwd-attr <WORD>
group-attr <WORD> group-filter <WORD> group-membership <WORD> {net-timeout} <1-10>
```

Parameters

[primary|secondary] host <A.B.C.D> port <1-65535> login <WORD> bind-dn <WORD> base-dn <WORD> passwd 0 <WORD> passwd-attr <WORD> group-attr <WORD> group-filter <WORD> group-membership <WORD> {net-timeout} <1-10>	• primary – Configures the primary LDAP server configuration • secondary – Configures the secondary LDAP server configuration The following configuration parameters are common for both the primary and secondary LDAP servers: • host – Configures LDAP server IP configuration • <A.B.C.D> – Specify the LDAP server IP address to configure • port <1-65535> – Select a value between 1 and 65535 to cofigure a port • login <WORD> – Specify a name to access the LDAP server. The maximum size is 127 • bind-dn <WORD> – Specify a distinguished bind name. The maximum bind-distingushed name size is 127 characters • base-dn <WORD> – Specify a name to configure base distinguished name. The maximum size is 127 characters • passwd [<0>|2|<WORD>] – Specify a name to configure LDAP server password. 0 specifies UNENCRYPTED password. 2 specifies ENCRYPTED password. The LDAP server bind password size is 31 • passwd-attr <WORD> – Specify a name to configure LDAP server password attribute. The maximum size is 63 characters • group-attr <WORD> – Specify a name to configure group attributes. The maximum size is 31 characters • group-filter <WORD> – Specify a name for the group-filter attribute. The maximum size is 255 characters • group-membership <WORD> – Specify a name for the group membership attribute. 63 is the maximum character size • {net-timeout} <1-10> – Select a value between 1 and 15 to configure network timeout value (number of seconds to wait for response of the server (network failures)

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#ldap-server primary host
172.16.10.19 port 162 login symbol bind-dn bind-dn1 base-dn base-dn1 passwd 0
motorola1 passwd-attr moto123 group-attr grop1 group-filter gropfilter1 group-
membership gropmember
ship1 net-timeout 2

rfs7000-37FABE(config-radius-server-policy-test)#ldap-server secondary host
172.16.10.2 port 2 login word bind-dn word1 base-
dn word2 passwd 0 word4 passwd-attr word4 group-attr word5 group-filter word6 group-
membership word8 net-timeout 3
rfs7000-37FABE(config-radius-server-policy-test)#

rfs7000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication data-source ldap
 crl-check
 ldap-server primary host 172.16.10.19 port 162 login symbol bind-dn bind-dn1 base-dn
base-dn1 passwd 0 motorola1 passwd-attr moto123 group-attr grop1 group-filter
gropfilter1 group-membership gropmembership1 net-timeout 2
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.5 local

radius-server-policy

Configures a local RADIUS realm

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
local realm <WORD>
```

Parameters

realm <WORD>	Configures a local RADIUS realm • <WORD> – Specify a local RADIUS realm name. Use a string up to 50 characters

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#local realm realm1
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.6 nas

radius-server-policy

Configures the key sent to a RADIUS client

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
nas <A.B.C.D/M> secret[0|2|<LINE>]
```

Parameters

<A.B.C.D/M> secret [0|2|<LINE>]	Sets the RADIUS client's IP address
	• secret – Sets the RADIUS client's shared secret
	  • 0 – Secret is specified UNENCRYPTED
	  • 2 – Secret is specified ENCRYPTED
	  • <LINE> – Defines the secret (client shared secret) up to 32 characters.

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#nas 172.16.10.10/24 key 0
wirelesswell
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.7 no

radius-server-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [authentication|clr-chesk|ldap-group-verification|
ldap-server|local|nas|proxy|session-resumption|use]
```

Parameters

[authentication|clr-chesk| ldap-group-verification| ldap-server|local| nas|proxy| session-resumption|use]	• authentication – Unconfigures RADIUS authentication • crl-check – Unconfigures a CRL check • ldap-group-verification – Disables LDAP group verification settings • ldap-server – Unconfigures LDAP server parameters • local – Unconfigures RADIUS local realm value • nas – Unconfigures the RADIUS client • proxy – Unconfigures the RADIUS proxy server • session-resumption – Disables session resumption

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#no use server-trustpoint
rfs7000-37FABE(config-radius-server-policy-test)#

rfs7000-37FABE(config-radius-server-policy-test)#no no local realm all
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.8 proxy

radius-server-policy

Configures a proxy RADIUS server based on the realm/suffix

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
proxy [realm|retry-count|retry-delay]
proxy realm <WORD> server <A.B.C.D> port <1024-65535> secret [0|2|<WORD>]
proxy retry-count <3-6>
proxy retry-delay retry-delay <5-10>]
```

Parameters

realm <WORD> server <A.B.C.D> port <1024-65535> secret 0 <WORD>	The realm name is a string up to 50 characters • server <A.B.C.D> – Specify an IP address to configure proxy server • port <1024-65535> – Select a value between 1024 and 65535 to configure proxy server port • secret [0|2|<WORD>] – Sets the proxy server secret string • 0 – Password is specified UNENCRYPTED • 2 – Password is specified ENCRYPTED • <WORD> – Specify the proxy server shared secret value
retry-count <3-6>	Select a value between 3 and 6 to configure the proxy server retry count
retry-delay <5-10>	Select a value between 5 and 10 seconds to configure the proxy server retry delay time

Usage Guidelines

Only five RADIUS proxy servers can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times the controller transmits each RADIUS request before giving up. The timeout value defines the duration for which the controller waits for a reply to a RADIUS request before retransmitting the request.

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#proxy realm test1 server 172.16.10.7
port 1025 secret 0 symbol123
rfs7000-37FABE(config-radius-server-policy-test)#

rfs7000-37FABE(config-radius-server-policy-test)#proxy retry-count 4
rfs7000-37FABE(config-radius-server-policy-test)#


rfs7000-37FABE(config-radius-server-policy-test)#proxy retry-delay 8
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.9 session-resumptionn

radius-server-policy

Enables session resumption/fast reauthentication by using cached attributes

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
session-resumption {life-time|max-entries}
session-resumption life-time  <1-24> {max-entries <10-1024>}
```

Parameters

{life-time|max-entries <10-1024>}	• life-time <1-24> – Sets the lifetime of cached entries • <1-24> – Sets the lifetime between 1 and 24 hours • max-entries <10-1024>} – Configures the maximum number of entries in the cache • <10-1024> – Sets the entries in the cache between 10 and 1024

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#session-resumption lifetime 10 max-
entries 11
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.2.10 use

radius-server-policy

Defines settings used with the RADIUS Server policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
use [radius-group <RAD-GROUP> {RAD-GROUP}|radius-user-pool-policy
<RAD-USER-POOL>]
```

Parameters

radius-group <RAD-GROUP> {RAD-GROUP}	Configures a RADIUS group (for LDAP users)
radius-user-pool-policy <RAD-USER-POOL>	Configures RADIUS user pool parameters. Specify a user name. It can be upto 32 characters

Example

```
rfs7000-37FABE(config-radius-server-policy-test)#use server-trustpoint name1
rfs7000-37FABE(config-radius-server-policy-test)#

rfs7000-37FABE(config-radius-server-policy-test)#use radius-user-pool-policy
testuser
rfs7000-37FABE(config-radius-server-policy-test)#
```

18.3 radius-user-pool-policy

Configures a RADIUS User Pool policy.

Use the (config) instance to configure RADIUS User Pool Policy related configuration commands. To navigate to the radius-user-pool-policy instance, use the following commands.

```
rfs7000-37FABE(config)#radius-user-pool-policy <pool name>
rfs7000-37FABE(config)#radius-user-pool-policy testuser
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

Table 18.3 Summarizes radius-user-pool policy commands

Table 18.3 *radius-user-pool-policy Commands*

Commands	Description	Reference
user	Configures RADIUS user parameters	*page 18-23*
no	Negates a command or sets its default value	*page 18-23*

18.3.1 user

radius-user-pool-policy

Configures RADIUS user parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
user <WORD> password [0|2|<WORD>] {group} RAD-GROUP {RAD-GROUP|guest}
user <WORD> password [0|2|<WORD>] {group} RAD-GROUP guest expiry-time <HH:MM> expiry-
date <MM:DD:YYY> {start-time}<HH:MM> start-date <MM:DD:YYYY>
```

Parameters

<WORD> password 0 <WORD> {group} RAD-GROUP {RAD-GROUP|guest expiry-time <HH:MM> expiry-date MM:DD:YYY {start-time} <HH:MM> start-date <MM:DD:YYYY>}	Enter a RADIUS user name up to 64 characters • password [0|2|<WORD>] – Enter RADIUS user password • 0 – Password is specified UNENCRYPTED • 2 – Password is specified ENCRYPTED • <WORD> – Enter a password (specified UNENCRYPTED) up to 21 characters in length • <WORD> – Enter a RADIUS user password to configure. It can be up to 21 characters length • {group} RAD-GROUP – Configures RADIUS server group configuration • RAD-GROUP – Specify an existing group name in the local database • guest – Enables guest user access • expiry-time <HH:MM> – Specify the expiry time for this user account in HH:MM format. For ex., 12:30 means 30 minutes after 12:00 the user login will expire • expiry-date <MM:DD:YYYY> – Specify time of expiry date for this user account in MM:DD:YYYY format. For ex. 12:15:2006 • start-time <HH:MM> – Specify user activation time in HH:MM format • start-date <MM:DD:YYYY> – Specify user access start-date in MM:DD:YYYY format

Example

```
rfs7000-37FABE(config-radius-user-pool-testuser)#user testuser password 0 symbol123
group test guest expiry-time 13:20 expiry-
date 12:15:2010 start-time 17:00 start-date 11:15:2010
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

18.3.2 no

radius-user-pool-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no user <WORD>
```

Parameters

user <WORD>	Deletes the existing RADIUS user configuration

Example

```
rfs7000-37FABE(config-radius-user-pool-testuser)#no user testuser
rfs7000-37FABE(config-radius-user-pool-testuser)#
```

CHAPTER 19 RADIO-QOS-POLICY

This chapter summarizes the radio-qos-policy in detail.

Use the (config) instance to configure radios-qos-policy related configuration commands. To navigate to the radio-qos-policy instance, use the following commands:

```
rfs7000-37FABE(config)#radio-qos-policy  <policy-name>
rfs7000-37FABE(config)#radio-qos-policy test
rfs7000-37FABE(config-radio-qos-test)#?
Radio QoS Mode commands:
  accelerated-multicast  Configure multicast streams for acceleration
  admission-control      Configure admission-control on this radio for one or
                         more access categories
  no                     Negate a command or set its defaults
  wmm                    Configure 802.11e/Wireless MultiMedia parameters

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs7000-37FABE(config-radio-qos-test)#
```

19.1 radio-qos-policy

Table 19.1 Summarizes radio-qos-policy commands

Table 19.1 *radio-qos-policy Commands*

Command	Description	Reference
accelerated-multicast	Configures multicast streams for acceleration	*page 19-3*
admission-control	Enables admission-control across all radios for one or more access categories	*page 19-4*
no	Negates a command or sets its default value	*page 19-6*
wmm	Configures 802.11e/wireless multimedia parameters	*page 19-7*

19.1.1 accelerated-multicast

radio-qos-policy

Configures multicast streams for acceleration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
accelerated-multicast [client-timeout <5-6000>|max-client-streams
 <1-4>|max-streams <0-256>|overflow-policy [reject|revert]|stream-threshold <1-500>]
```

Parameters

client-timeout <5-6000>	Configure a timeout for clients between 5 and 6000
max-client-streams <1-4>	Configures the maximum number of accelerated multicast streams per client. The default value is 2.
max-streams <0-256>	Configures maximum number of accelerated multicast streams per radio. The default value is 25.
overflow-policy [reject|revert]	Configures policy to follow in case too many clients register • reject – Rejects new clients • revert – Reverts to regular multicast delivery
stream-threshold <1-500>	Configures packets per second for streams to accelerate. The default value is 30.

Example

```
rfs7000-37FABE(config-radio-qos-test)#accelerated-multicast stream-threshold 15
rfs7000-37FABE(config-radio-qos-test)#
```

19.1.2 admission-control

radio-qos-policy

Enables admission control across all radios for one or more access categories

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
admission-control [background|best-effort|firewall-detected-traffic|implicit-
tspec|video|voice]
admission-control [background|best-effort|video|voice] {max-airtime-percent <0-150>
|max-clients <0-256> |max-roamed-clients <0-256>|
 reserved-for-roam-percent <0-150>}
```

Parameters

[background|best-effort| firewall-detected-traffic| implicit-tspec|video|voice]	• background – Configures background access category admission control parameters • best-effort – Configures best effort access category admission control parameters • video – Configures video access category admission-control parameters • voice – Configures voice access category admission-control parameters The following parameters are common for the above: • max-airtime-percent<0-150> – Specifies the maximum percentage of airtime for this access category • <0-150> – Select a value between 0 and 150 to calculate the percentage of air-time (including oversubscription) • max-clients – Specifies the maximum number of wireless clients admitted • <0-256> – Select the maximum number of wireless clients admitted to this access category • max-roamed-clients <0-256> – Specifies the maximum number of roaming wireless clients admitted to this access category • <0-256> – Select the maximum number of roaming wireless devices admitted to this access category • reserved-for-roam-percent <0-150> – Calculates the percentage of air time allocated exclusively for roamed wireless-clients. This value is calculated relative to the configured max air time for this access category • <0-150> – Select a value between 0 and 150 to calculate a percentage for air-time (including oversubscription) • firewall-detected-traffic – Enforces admission control for traffic whose access category is detected by the firewall ALG (Eg: SIP voice calls) • implicit-tspec – Enables implicit traffic-specifiers for clients that do not support WMM-TSPEC but are accessing admission controlled access categories

Example

```
rfs7000-37FABE(config-radio-qos-test)#admission-control best-effort max-mus 7
rfs7000-37FABE(config-radio-qos-test)#

rfs7000-37FABE(config-radio-qos-test)#admission-control voice reserved-for-roam-
percent 8
rfs7000-37FABE(config-radio-qos-test)#

rfs7000-37FABE(config-radio-qos-test)#admission-control voice max-airtime-percent 9
rfs7000-37FABE(config-radio-qos-test)#
```

19.1.3 no

radio-qos-policy

Negates a command or sets its default value

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [accelerated-multicast|admission-control|wmm]
```

Parameters

[admission-control| wmm]	• accelerated-multicast – Unconfigures multicast streams for acceleration • admission-control – Unconfigures admission-control on the radio for one or more access categories • wmm – Unconfigures 802.11e/wireless multimedia parameters

Example

```
rfs7000-37FABE(config-radio-qos-test)#no admission-control best-effort enable
rfs7000-37FABE(config-radio-qos-test)#
```

19.1.4 wmm

radio-qos-policy

Configures 802.11e/Wireless MultiMedia parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wmm [background|best-effort|video|voice] [aifsn <1-15>
|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]
```

Parameters

[background|best-effort video|voice] [aifsn|cw-max| cw-mintxop-limit]	• background – Configures background access category parameters • best-effort – Configures best effort access category parameters • video – Configures video access category parameters • voice – Configure voice access category parameters The following parameters are common for all the above: • aifsn <1-15> – Configures the arbitration inter frame spacing number (AIFSN) as the wait time between data frames is derived from the AIFSN and slot-time • <1-15> – Select a value between 1 and 15 to configure the (AIFSN) • cw-max <0-15> – Maximum contention window: Clients pick a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Sets a value from 0-15. • cw-min – Minimum contention window: Clients select a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0-15. • txop-limit <0-65535> – Configures the transmit-opportunity: (the interval of time during which a particular client has the right to initiate transmissions) • <0-65535> – Select a value between 0 and 65535 to configure the transmit-opportunity in 32 microsecond units

Example

```
rfs7000-37FABE(config-radio-qos-test)#wmm best-effort aifsn 7
rfs7000-37FABE(config-radio-qos-test)#

rfs7000-37FABE(config-radio-qos-test)#wmm voice txop-limit 1
rfs7000-37FABE(config-radio-qos-test)#
```

NOTE: The commands clrscr, commit, exit, end, help, write, revert, service and show are common commands. For more information, see *Chapter 5, COMMON COMMANDS*.

CHAPTER 20 ROLE-POLICY

This chapter summarizes Role Policies in detail.

Use the (config-role-policy) instance to configure role-policy related configuration commands. To navigate to the config-role instance, use the following commands:

```
rfs7000-37FABE(config)#role-policy <policy-name>
rfs7000-37FABE(config)#role-policy role1
rfs7000-37FABE(config-role-policy-role1)# ?
Role Policy Mode commands:
  default-role  Configuration for Wireless Clients not matching any role
  no            Negate a command or set its defaults
  user-role     Create a role

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

rfs7000-37FABE(config-role-policy-role1)#
```

20.1 role-policy

Table 20.1 Summarizes role-policy commands

Table 20.1 *role-policy commands*

Command	Description	Reference
default-role	When a client fails to find a matching role, the default-role action is assigned to that client	*page 20-3*
no	Negates a command or sets its default value	*page 20-4*
user-role	Creates a role and associates it to the newly created role policy	*page 20-5*

20.1.1 default-role

role-policy

When a client fails to find a matching role, the default role action is assigned to that client.

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
default-role use [ip-access-list|mac-access-list]
default-role use ip-access-list [in|out] <IP-ACCESS-LIST> precedence
<1-100>
default-role use mac-access-list [in|out] <MAC-ACCESS-LIST> precedence
<1-100>
```

Parameters

use ip-access-list [in|out] <IP-ACCESS-LIST> precedence <1-100>	Uses an IP access-list • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets The following parameters are common for the above: • <IP-ACCESS-LIST> – Specifies the access list name • precedence – Based on the packets received, the lower precedence value is evaluated first • <1-100> – Specifies a precedence value between 1 and 100
use mac-access-list [in|out] <MAC-ACCESS-LIST> precedence <1-100>	Uses a MAC access-list • in – Applies the rule to the incoming packets • out – Applies the rule to the outgoing packets The following parameters are common for the above: • <MAC-ACCESS-LIST> – Specifies the access-list name • precedence <1-100> – Based on the packets received, the lower precedence value is evaluated first • <1-100> – Specifies the precedence value between 1 and 100

Example

```
rfs7000-37FABE(config-role-policy-test)#default-role use ip-access-list in test
precedence 1
rfs7000-37FABE(config-role-policy-test)#

rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#show role wireless-clients on
rfs7000-37FABE
Role: role1, precedence 1
No ROLE statistics found.
rfs7000-37FABE(config-device-00-15-70-37-FA-BE)#
```

20.1.2 no

role-policy

Negates a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [default-role|user-role]
```

Parameters

default-role	Deletes default role action
role	Deletes a role

Example

```
rfs7000-37FABE(config-role-policy-test)#no default-role use ip-access-list in test
precedence 1
rfs7000-37FABE(config-role-policy-test)#

rfs7000-37FABE(config-role-policy-test)#show context
role-policy test
 role role1 precedence 1
rfs7000-37FABE(config-role-policy-test)#
```

20.1.3 user-role

role-policy

Creates a role and associates it to the newly created role-policy

```
rfs7000-37FABE(config-role-policy-test)#user- role <role-name> precedence <1-10000>
rfs7000-37FABE(config-role-policy-test)# user-role role1 precedence 1

rfs7000-37FABE(config-role-role1)#
```

Table 20.2 Summarizes role commands

Table 20.2 *user-role Commands*

Commands	Description	Reference
ap-location	Sets the AP's location	*page 20-6*
authentication-type	Selects an authentication type for the role	*page 20-7*
captive-portal	Defines a captive portal role based filter	*page 20-8*
encryption-type	Selects the encryption type	*page 20-9*
group	Sets group configuration for the role	*page 20-10*
mu-mac	Configures the client MAC addresses for role based firewall	*page 20-11*
no	Negates a command or sets its default values	*page 20-12*
ssid	Specifies SSID configuration	*page 20-13*
use	Defines the settings used with the role policy	*page 20-14*

20.1.3.1 ap-location

user-role

Sets the AP location

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap-location [any|contains|exact|not-contains]
ap-location any
ap-location contains <WORD>
ap-location exact <WORD>
ap-location not-contains <WORD>
```

Parameters

any	Defines any AP location
contains <WORD>	AP location contains the specified string
exact <WORD>	AP location contains the exact specified string
not-contains <word>	AP location does not contain the string

Example

```
rfs7000-37FABE(config-role-role1))#ap-location any
rfs7000-37FABE(config-role-role1))#

rfs7000-37FABE(config-role-role1))#ap-location contains office
rfs7000-37FABE(config-role-role1))#
```

20.1.3.2 authentication-type

user-role

Selects the authentication type for the role

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
authentication-type [any|eq|neq]
authentication-type any
authentication-type eq [eap|kerberos|mac-auth|none]
authentication-type neq[eap|kerberos|mac-auth|none]
```

Parameters

any	The authentication type can be any one from the listed options
eq [eap|kerberos| mac-auth|none]	The authentication type equals any one of the following types: • eap – Extensible authentication protocol • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used
neq [eap|hotspot|kerberos| mac-auth|none]	The authentication protocol does not contain one of the listed options

Example

```
rfs7000-37FABE(config-role-role1))#authentication-type eq kerberos
rfs7000-37FABE(config-role-role1))#
```

20.1.3.3 captive-portal

user-role

Defines a captive portal based role filter

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
captive-portal authentication-state [any|post-login|pre-login]
```

Parameters

authentication-state [any|post-login|pre-login]	Defines authentication state of wireless client associated to captive portal • any – Specifies any authentication state • post-login – Specifies authentication is completed successfully • pre-login – Specifies authentication is pending

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-role1)#captive-portal
authentication-state pre-login
rfs7000-37FABE(config-role-policy-test-user-role-role1)#

rfs7000-37FABE(config-role-policy-test-user-role-role1)# show context
 user-role role1 precedence 1
  captive-portal authentication-state pre-login
rfs7000-37FABE(config-role-policy-test-user-role-role1)#
```

20.1.3.4 encryption-type

user-role

Selects the encryption type used for the role

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
encryption-type [any|eq|neq]
encryption-type any
encryption-type eq [ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep64] {ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep64}
encryption-type neq [ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep64] {ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep64}
```

Parameters

any	The encryption type can be any one of the listed options
eq [ccmp|keyguard|none|tkip| wep128|wep64]	The encryption type equals one of the following: • ccmp • keyguard • none • tkip • tkip-ccmp • wep128 • wep128-keyguard • wep128-keyguard • wep64
neq[ccmp|keyguard|none|tkip| wep128|wep64]	The encryption type must not be one of the listed options

Example

```
rfs7000-37FABE(config-role-role1))#encryption-type eq ccmp
rfs7000-37FABE(config-role-role1))#
```

20.1.3.5 group

user-role

Sets the group configuration for the role

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
group [any|contains|exact|not-contains]
group any
group contains <WORD>
group exact <WORD>
group not-contains <WORD>
```

Parameters

any	Specifies any group
contains <WORD>	Group contains the specified string
exact <WORD>	Group contains the exact specified string
not-contains <word>	Group does not contain the specified string

Example

```
rfs7000-37FABE(config-role-role1))#group any
rfs7000-37FABE(config-role-role1))#
```

20.1.3.6 mu-mac

user-role

Configures the client's MAC addresses for the role based firewall

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mu-mac [<MAC Address> <Mask> <MAC Address> |any]
```

Parameters

<MAC Address>	The address of the allowed client. The MAC address can be in the format of AA-BB-CC-DD-EE-FF
<MAC Address> <Mask>	The address and mask combination for the allowed client. <MAC Address> and <Mask> should be in the format of AA-BB-CC-DD-EE-FF
any	Match with any MAC address

Example

```
rfs7000-37FABE(config-role-role1))#mu-mac 11-22-33-44-55-66 mask 44-55-66-77-88-99 ?

rfs7000-37FABE(config-role-role1))#mu-mac any
rfs7000-37FABE(config-role-role1))#
```

20.1.3.7 no

user-role

Negates a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [ap-location|authentication-type|captive-portal|
encryption-type|group|mu-mac|ssid|use]
```

Parameters

None

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-role-policy-role1-user-role-role1)#no group
rfs7000-37FABE(config-role-policy-role1-user-role-role1)#

rfs7000-37FABE(config-role-policy-role1-user-role-role1)#no ap-location
rfs7000-37FABE(config-role-policy-role1-user-role-role1)#
```

20.1.3.8 ssid

user-role

Specifies the SSID configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ssid [any|exact|contains|not-contains]
ssid [exact|contains|not-contains] <WORD>
```

Parameters

[any|exact|contains| not-contains]	• any – Specifies that the SSID can be any value • contains <WORD> – Specifies SSID contains the given string • exact – Specifies SSID exactly matches with the given string • not-contains – Specifies SSID does not contain the given string • <WORD> – Specify the string to match against - case sensitive (compared against SSID configured under WLAN)

Example

```
rfs7000-37FABE(config-role-policy-test-user-role-role1)#ssid not-contains TESTSSID
rfs7000-37FABE(config-role-policy-test-user-role-role1)#
```

20.1.3.9 use

user-role

Defines the settings used with the user role

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
use [ip-access-list|mac-access-list]
use ip-access-list [in|out] <IP-ACCESS-LIST> precedence
<1-100>
use mac-access-list [in|out] <MAC-ACCESS-LIST> precedence <1-100>
```

Parameters

ip-access-list [in|out] <IP-ACCESS-LIST> precedence <1-100>	Uses an IP access list • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets The following parameters are common for the above: • <IP-ACCESS-LIST> – Specifies the access list name • precedence – Based on the packets received, the lower precedence value is evaluated first • <1-100> – Specifies the precedence value between 1 and 100
mac-access-list [in|out] <MAC-ACCESS-LIST> precedence <1-100>	Uses a MAC access list • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets The following parameters are common for the above: • <MAC-ACCESS-LIST> – Specifies the access list name • precedence – Based on the packets received, the lower precedence value is evaluated first • <1-100> – Specifies the precedence value is from 1 -100

Example

```
rfs7000-37FABE(config-role-role1)#use ip-access-list in test precedence 9
rfs7000-37FABE(config-role-role1)#
```

NOTE: The commands no, write, clrscr, commit, exit, help, show, service are common commands. For more information, see *Chapter 5, COMMON COMMANDS*.

CHAPTER 21 SMART-RF-POLICY

This chapter summarizes Smart RF Policy commands within the CLI structure.

Use the (config) instance to configure Smart RF Policy related configuration commands. To navigate to the smart-rf-policy instance, use the following commands:

```
rfs7000-37FABE(config)#smart-rf-policy <policy name>
rfs7000-37FABE(config)#smart-rf-policy test
rfs7000-37FABE(config-smart-rf-policy-test)#?
Smart RF Mode commands:
  assignable-power         Specify the assignable power during power-assignment
  auto-assign-sensor       Allow smart-rf to select optimal sensor radios for
                           wips and unauthorized ap detection
  channel-list             Select channel list for smart-rf
  channel-width            Select channel width for smart-rf
  coverage-hole-recovery   Recover from coverage hole
  enable                   Enable this smart-rf policy
  group-by                 Configure grouping parameters
  interference-recovery    Recover issues due to excessive noise and
                           interference
  neighbor-recovery        Recover issues due to faulty neighbor radios
  no                       Negate a command or set its defaults
  sensitivity              Configure smart-rf sensitivity (Modifies various
                           other smart-rf configuration items)
  smart-ocs-monitoring     Smart off channel scanning

  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal

rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1 smart-rf-policy

Table 21.1Summarizes Smart RF Policy commands

Table 21.1 *smart-rf-policy Commands*

Command	Description	Reference
assignable-power	Specifies the power range during power assignment	*page 21-3*
auto-assign-sensor	Allows Smart RF to select optimal sensor radios for WIPS and unauthorized AP detection	*page 21-4*
channel-list	Assigns the channel list for the selected frequency	*page 21-5*
channel-width	Selects the channel width for Smart RF configuration	*page 21-6*
coverage-hole-recovery	Enables recovery from coverage-hole errors	*page 21-7*
enable	Enables the configured Smart RF Policy settings	*page 21-8*
group-by	Configures grouping parameters	*page 21-9*
interference-recovery	Recovers issues due to excessive noise and interference	*page 21-10*
neighbor-recovery	Enables recovery from errors due to faulty neighbor radios	*page 21-11*
no	Negates a command or sets its default values	*page 21-12*
sensitivity	Configures Smart RF sensitivity	*page 21-13*
smart-ocs-monitoring	Applies smart off channel scanning instead of dedicated detectors	*page 21-14*

21.1.1 assignable-power

smart-rf-policy

Specifies the power range during power assignment

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
assignable-power [2.4Ghz|5Ghz] [max|min] <1-20>
```

Parameters

[2.4Ghz|5Ghz] [max|min] <1-20>	[2.4Ghz|5Ghz] [max|min] <1-20> – Specifies the power range during power assignment • max <1-20> – Sets the upper bound of the power range. The value is between 1 and 20 • min <1-20> – Sets the lower bound of the power range. The value is between 1 and 20

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#assignable-power 5Ghz min 8
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.2 auto-assign-sensor

smart-rf-policy

Allows Smart RF to select optimal sensor radios for WIPS and unauthorized AP detection

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Parameters

None

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#auto-assign-sensor
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.3 channel-list

smart-rf-policy

Assigns the channel list for the selected frequency

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
channel-list [2.4Ghz|5Ghz] <WORD>
```

Parameters

[2.4Ghz|5Ghz] <WORD>	Assigns the channel list for the selected frequency • <WORD> – A comma separated list of channel numbers

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#channel-list 2.4Ghz 1,12
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.4 channel-width

smart-rf-policy

Selects the channel width for Smart RF configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
channel-width [2.4Ghz|5Ghz] [20Mhz|40Mhz|auto]
```

Parameters

[2.4Ghz|5Ghz] [20Mhz|40Mhz|auto]	Assigns the channel width for the selected frequency • 20Mhz – Assigns the 20Mhz channel width • 40Mhz – Assigns the 40Mhz channel width • auto – Assigns the best possible channel in the 20/40Mhz width

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#channel-width 5 auto
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#channel-width 5 40Mhz
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.5 coverage-hole-recovery

smart-rf-policy

Enables recovery from coverage hole errors

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
coverage-hole-recovery {client-threshold|coverage-interval|interval|
snr-threshold}
coverage-hole-recovery client-threshold [2.4Ghz|5Ghz] <1-255>
coverage-hole-recovery [coverage-interval|interval] [2.4Ghz|5Ghz] <1-120>
coverage-hole-recovery snr-threshold [2.4Ghz|5Ghz]  <1-75>
```

Parameters

client-threshold|coverage-interval|interval| snr-threshold}	• client-threshold <1-255> – Specifies the minimum number of clients below SNR threshold required for coverage hole recovery. Select the number of clients between 1 and 255. • coverage-interval <1-120> – Specify the interval at which recovery should be performed after coverage hole is discovered. Select a interval coverage- interval value between 1 and 120 seconds • interval <1-120> – Specify the interval at which a coverage hole recovery should be performed before coverage hole is detected. Select a interval value between 1 and 120 seconds • snr-threshold <1-75> – Specify the SNR threshold below which coverage recovery is initiated. Select a SNR threshold value between 1 and 75 The following bandwidth is common for all the above: • 2.4GHz – 2.4GHz band • 5GHz – 5GHz band

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#coverage-hole-recovery snr-threshold
5GHz 1

rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.6 enable

smart-rf-policy

Enables the configured Smart RF policy settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
enable
```

Parameters

None

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#enable
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 enable
 calibration wait-time 4
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.7 group-by

smart-rf-policy

Configures grouping parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
group-by [building|floor]
```

Parameters

[building|floor]	• building – Configures a group based on building • floor – Configures a group based on floor

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#group-by floor
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.8 interference-recovery

smart-rf-policy

Recovers detected problems due to excessive noise and interference

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
interference-recovery {channel-hold-time <0-86400> |channel-switch-delta
[2.4Ghz|5Ghz] <5-35>|client-threshold <1-255>|interference|noise}
```

Parameters

channel-hold-time <0-86400>	Defines the minimum time between two channel change recoveries • <0-86400> – Sets the time between channel change assignments based on interference/noise in seconds
channel-switch-delta [2.4Ghz|5Ghz] <5-35>	Specifies the difference between the current and best channel interference for a channel change • 2.4Ghz|5Ghz] <5-35> – Select the bandwidth as 2.4Ghz or 5Ghz • <5-35> – Specify the difference in dbm by selecting a value between 5 and 35
interference	Considers the external interference values for performing interference recovery
noise	Considers the noise values for performing interference recovery
client-threshold <1-255>	Specifies client thresholds associated after which, a channel change due to interference recovery is avoided • <1-255> – Specify the number of clients between 1 and 255

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#interference-recovery channel-switch-
delta 5 5
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#interference-recovery interference
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#interference-recovery retry-threshold
0.9
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.9 neighbor-recovery

smart-rf-policy

Enables a recovery from errors due to faulty neighbor radios

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
neighbor-recovery {power-hold-time <0-3600>|power-threshold} [2.4Ghz|5Ghz]
<-85--55>
```

Parameters

power-hold-time <0-3600>	Specifies the minimum time between two power change recoveries • <0-3600> – Sets the time between 0 and 3600 seconds
{power-threshold} [2.4Ghz|5Ghz] <-85--55>	Specifies the power threshold based on the recovery performed • [2.4Ghz|5Ghz] <-85--55> – Select the band width as 2.4 Dez or 5Ghz • <-85--55> – Select a threshold value between -85 and -55 dbm

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#neighbor-recovery power-threshold 2.4 -
82
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#neighbor-recovery power-threshold 5 -65
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.10 no

smart-rf-policy

Negates a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [assignable-power|auto-assign|calibration|
channel-list|channel-width|coverage-hole-recovery|enable|
group-by|interference-recovery|neighbor-recovery|
smart-ocs-monitoring]
```

Parameters

[assignable-power| auto-assign|calibration| channel-list| channel-width| coverage-hole-recovery|enable| hold-time| interference-recovery| neighbor-recovery| smart-ocs-monitoring]	• assignable-power – Negates the power range assignment • auto-assign – Disables all auto assignment features • calibration – Resets calibration parameters • channel-list – Removes the assigned channel-list for the selected frequency • channel-width – Removes the assigned channel-width for the selected frequency • coverage-hole-recovery – Disables recovery from coverage hole errors • enable – Disables the Smart RF policy feature • group-by – Unconfigures grouping parameters • interference-recovery – Disables recovery issues caused by excessive noise and interference • neighbor-recovery – Disables recovery issues caused by faulty neighbor radios • smart-ocs-monitoring – Disables the off channel monitoring feature

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#no assignable-power 5Ghz min
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#no smart-ocs-monitoring frequency 2.4Ghz
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.11 sensitivity

smart-rf-policy

Configures Smart-RF sensitivity

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
sensitivity [custom|high|low|medium]
```

Parameters

[custom|high|low|medium]	Configures Smart-RF sensitivity • Custom – Custom sensitivity • high – High sensitivity • low – low sensitivity • medium – Medium sensitivity

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#sensitivity medium
rfs7000-37FABE(config-smart-rf-policy-test)#
```

21.1.12 smart-ocs-monitoring

smart-rf-policy

Applies smart off channel scanning instead of dedicated detectors

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
smart-ocs-monitoring {extended-scan-frequency|frequency|
off-channel-duration|sample-count}
```

Parameters

{extended-scan-frequency|frequency|off-channel-duration|sample-count}	• extended-scan-frequency [2.4Ghz|5Ghz] <0-50> – Specifies the frequency at which an extended scan is performed instead of a neighbor only scan. Sets the number of trails from 0-50. • frequency [2.4Ghz|5Ghz] <1-120> – Specifies the frequency at which the channel has to be switched. Sets the value in seconds from 1-120. • off-channel-duration [2.4Ghz|5Ghz] <20-150> – Specifies the duration required to spend off channel. Sets the value in milliseconds from 20-150 • sample-count [2.4Ghz|5Ghz] <1-120> – Specifies the number of samples collected before reporting to the Smart-RF master. Sets the sample-count from 1-120.

Example

```
rfs7000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring extended-scan-
frequency 2.4Ghz 9
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring sample-count 2.4Ghz
3
rfs7000-37FABE(config-smart-rf-policy-test)#

rfs7000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring off-channel-
duration 2.4Ghz 25
rfs7000-37FABE(config-smart-rf-policy-test)#
```

NOTE: The commands clrscr, commit, end, exit, help, revert, service, show, write are common commands across all chapters. For more information, see *Chapter 5, COMMON COMMANDS*.

CHAPTER 22 WIPS-POLICY

This chapter summarizes WIPS-Policy in detail.

Use the (config) instance to configure wips-policy related configuration commands. To navigate to the WIPS-Policy instance, use the following commands:

```
rfs7000-37FABE(config)#wips-policy  <policy-name>
rfs7000-37FABE(config)#wips-policy  test
rfs7000-37FABE(config-wips-policy-test)#?
Wips Policy Mode commands:
  ap-detection                Unsanctioned AP detection
  enable                      Enable this wips policy
  event                       Configure an event
  history-throttle-duration  Configure the duration for which event duplicates are not
stored in history
  no                          Negate a command or set its defaults
  signature                   Signature to configure
  use                         Set setting to use

  clrscr                      Clears the display screen
  commit                      Commit all changes made in this session
  do                          Run commands from Exec mode
  end                         End current mode and change to EXEC mode
  exit                        End current mode and down to previous mode
  help                        Description of the interactive help system
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  write                       Write running configuration to memory or terminal

rfs7000-37FABE(config-wips-policy-test)#
```

22.1 wips-policy

Table 22.1 Summarizes WIPS-Policy commands in detail

Table 22.1 *wips-policy Commands*

Command	Description	Reference
ap-detection	Defines ap-detection configuration	*page 22-3*
enable	Enables wips-policy	*page 22-4*
event	Configures events	*page 22-5*
history-throttle-duration	Configures the duration event duplicates are not stored in history	*page 22-8*
no	Negates a command or sets its default values	*page 22-9*
signature	Configures signature	*page 22-11*
use	Defines the settings used with the WIPS policy	*page 22-10*

22.1.1 ap-detection

wips-policy

Defines ap-detection configuration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ap-detection {age-out <30-86400>|wait-time <10-600>}
```

Parameters

age-out <30-86400>	Configures the ageout time between 30-86400 seconds
wait-time <10-600>	Configures the wait time between 10-600 seconds

Example

```
rfs7000-37FABE(config-wips-policy-test)#ap-detection wait-time 15
rfs7000-37FABE(config-wips-policy-test)#

rfs7000-37FABE(config-wips-policy-test)#ap-detection age-out 50
rfs7000-37FABE(config-wips-policy-test)#
```

22.1.2 enable

wips-policy

Enables wips-policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
enable
```

Parameters

enable	Enables a WIPS policy

Example

```
rfs7000-37FABE(config-wips-policy-test)#enable
rfs7000-37FABE(config-wips-policy-test)#
```

22.1.3 event

wips-policy

Configures an event

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
event [ap-anomaly|client-anomaly|enable-all-events|excessive]

event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-
beacon|asleap||impersonation-attack|null-probe-response|transmitting-device-using-
invalid-mac|unencrypted-wired-leakage|wireless-bridge]

event client-anomaly [crackable-wep-iv-key-used|dos-broadcast-deauth|fuzzing-all-
zero-macs|fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-
seq-num|identical-src-and-dest-addr|invalid-8021x-frames| netstumbler-generic|non-
changing-wep-iv|tkip-mic-counter-measures|wellenreiter]{filter-ageout <0-86400>}]

event excessive [80211-replay-check-failure| aggressive-scanning|auth-     server-
failures|decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm |dos-
unicast-deauth-or-disassoc|eap-flood|eap-nak-flood  |frames-from-unassoc-station]
{filter-ageout <0-86400>|threshold-client <0-65535> |threshold-radio <0-65535>}
```

Parameters

ap-anomaly [ad-hoc-violation|airjack| ap-ssid-broadcast-in-beacon|asleap|impersonation-attack|null-probe-response| transmitting-device-using-invalid-mac| unencrypted-wired-leakage|wireless-bridge]	Configures ap-anomaly type events • ad-hoc-violation – Ad-Hoc network violation • airjack – AirJack attack • ap-ssid-broadcast-in-beacon – AP SSID broadcast in beacon • asleap – ASLEAP attack • impersonation-attack – Impersonation attack detected • null-probe-response – Null probe response • transmitting-device-using-invalid-mac – Transmitting device using invalid MAC • unencrypted-wired-leakage – Unencrypted wired leakage detected • wireless-bridge – Wireless Bridge (WDS) frames detected
client-anomaly[crackable-wep-iv-key-used|dos-broadcast-deauth| fuzzing-all-zero-macs|fuzzing-invalid-frame-type| fuzzing-invalid-mgmt-frames| fuzzing-invalid-seq-num|identical-src-and-dest-addr| invalid-8021x-frames| netstumbler-generic| non-changing-wep-iv|tkip-mic-counter-measures|wellenreiter] {filter-agetimeout <0-86400>}	Configures client-anomaly type events • crackable-wep-iv-key-used – Crackable WEP IV Key Used • dos-broadcast-deauth – DoS broadcast deauthentication • fuzzing-all-zero-macs – Fuzzing: All zero MAC address observed • fuzzing-invalid-frame-type – Fuzzing:invalid frame type detected • fuzzing-invalid-mgmt-frames – Fuzzing: invalid management frame • fuzzing-invalid-seq-num – Fuzzing: invalid sequence number • identical-src-and-dest-addr – Identical source and destination addresses • invalid-8021x-frames – Fuzzing: Invalid 802.1x frames detected • netstumbler-generic – Netstumbler (v3.2.0, 3.2.3, 3.3.0) • non-changing-wep-iv – Non-changing WEP IV • tkip-mic-counter-measures – TKIP MIC counter measures caused by station • wellenreiter – Wellenreiter The following parameters are common for all the above: • {filter-ageout <0-86400>} – Configures filter-ageout • <0-86400> – Configures filter-ageout values between 0 and 86400 seconds

enable-all-events	Enables all events

excessive [80211-replay-check-failure| aggressive-scanning|auth-server-failures| decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm|dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood |frames-from-unassoc-station] {filter-ageout <0-86400>|threshold-mu <0-65535>|threshold-radio <0-65535>	Configures excessive type events
	• 80211-replay-check-failure – 802.11replay check failure
	• aggressive-scanning – Aggressive scanning
	• auth-server-failures – Failures reported by authentication servers
	• decryption-failures – Decryption failures
	• dos-assoc-or-auth-flood – DoS association or authentication flood
	• dos-eapol-start-storm – DoS EAPOL-start storm
	• dos-unicast-deauth-or-disassoc – DoS association or authentication flood
	• eap-flood – EAP flood
	• eap-nak-flood – EAP-NAK flood
	• frames-from-unassoc-station – Frames from unassociated stations
	The following parameters are common for all the above:
	• {filter-ageout <0-86400>} – Configures filter-ageout
	  • <0-86400> – Configures filter-ageout values between 0 and 86400 seconds
	• threshold-client <0-65535> – Configures threshold-client
	  • <0-65535> – Configures wireless client threshold limit for 60 seconds
	• threshold-radio <0-65535> – Configures Radio threshold configuration
	  • <0-65535> – Radio threshold limit for 60 seconds

Example

```
rfs7000-37FABE(config-wips-policy-test)#event enable-all-events
rfs7000-37FABE(config-wips-policy-test)#
rfs7000-37FABE(config-wips-policy-test)#event excessive 80211-replay-check-failure
filter-ageout 9 threshold-client 8 threshold-radio 99
rfs7000-37FABE(config-wips-policy-test)#

rfs7000-37FABE(config-wips-policy-test)#event client-anomaly wellenreiter filter-
ageout 99
rfs7000-37FABE(config-wips-policy-test)#
```

22.1.4 history-throttle-duration

wips-policy

Configures the duration where event duplicates are not stored in the history

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
history-throttle-duration <30-86400>
```

Parameters

history-throttle-duration <30-86400>	Configures the duration event duplicates are not stored in the history • <30-86400> – Configures the duration in seconds

Example

```
rfs7000-37FABE(config-wips-policy-test)#history-throttle-duration 77
rfs7000-37FABE(config-wips-policy-test)#
```

22.1.5 no

wips-policy

Negates a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [ap-detection|enable|event|history-throttle-duration|signature|use]
```

Parameters

None

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-wips-policy-test)#no enable
rfs7000-37FABE(config-wips-policy-test)#

rfs7000-37FABE(config-wips-policy-test)#no ap-detection
rfs7000-37FABE(config-wips-policy-test)#


rfs7000-37FABE(config-wips-policy-test)#no history-throttle-duration
rfs7000-37FABE(config-wips-policy-test)#
```

22.1.6 use

wips-policy

Defines the settings used with the WIPS policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP650
- AP71xx
- AP6511
- AP6532

Syntax

```
use device-categorization <DEVICE-CATEGORIZATION>
```

Parameters

device-categorization <DEVICE-CATEGORIZATION>	Configures the device categorization list • <DEVICE-CATEGORIZATION> – Specify the device categorization object name to be associated with this profile

Example

```
rfs7000-37FABE(config-wips-policy-test)#use device-categorization rfs7000
rfs7000-37FABE(config-wips-policy-test)#

rfs7000-37FABE(config-wips-policy-test)#show context
wips-policy test
 no enable
 signature test
  src-mac 11-22-33-44-55-66
 signature testsignature
 ap-detection-ageout 35
 ap-detection-wait-time 15
 use device-categorization rfs7000
rfs7000-37FABE(config-wips-policy-test)#
```

22.1.7 signature

wips-policy

Defines the signature

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP650
- AP71xx
- AP6511
- AP6532

Syntax

```
signature <signature-name>
```

Parameters

signature <signature-name>	Configures signature • <signature-name> – Specify the signature name to be configured

Example

```
rfs7000-37FABE(config-wips-policy-test)#signature symbol
rfs7000-37FABE(config-test-signature-symbol)#
```

NOTE: Please refer *signature-mode commands* for signature-mode related commands.

Table 22.2 Summarizes signature commands

Table 22.2 *signature-mode commands*

Commands	Description	Reference
bssid	Configures bssid MAC address	*page 22-13*
dst-mac	Configures destination MAC address	*page 22-14*
filter-ageout	Configures filter-ageout	*page 22-15*
frame-type	Configures frame-type to match	*page 22-16*
mode	Enables/Disables signature mode	*page 22-17*
payload	Configures payload settings	*page 22-18*
src-mac	Configures source MAC address	*page 22-19*

Table 22.2 *signature-mode commands*

Commands	Description	Reference
ssid-match	Configures the match based on SSID	*page 22-20*
threshold-client	Configures the wireless client threshold limit	*page 22-21*
threshold-radio	Configures radio threshold limit	*page 22-22*
no	Negates a command or sets its default values	*page 22-23*

22.1.7.1 bssid

signature

Configures BSSID MAC address

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
bssid <MAC Address>
```

Parameters

bssid <MAC Address>	Configures BSSID MAC address • <MAC Address> – Specify the MAC address to match

Example

```
rfs7000-37FABE(config-test-signature-symbol)#bssid 11-22-33-44-55-66
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.2 dst-mac

signature

Configures destination MAC address

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
dst-mac <MAC Address>
```

Parameters

dst-mac <MAC Address>	Configures destination MAC address • <MAC Address> – Specify the MAC address to match

Example

```
rfs7000-37FABE(config-test-signature-symbol)#dst-mac 11-22-33-44-55-66
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.3 filter-ageout

signature

Configures the filter ageout in seconds

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
filter-ageout <1-86400>
```

Parameters

filter-ageout <1-86400>	Configures filter-ageout • <1-86400> – Specify the filter ageout in seconds

Example

```
rfs7000-37FABE(config-test-signature-symbol)#filter-ageout 8
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.4 frame-type

signature

Configures frame-type to match

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
frame-type [all|assoc|auth|beacon|data|deauth|disassoc|
  mgmt|probe-req|probe-resp|reassoc]
```

Parameters

frame-type [all|assoc| auth|beacon|data| deauth|disassoc|mgmt| probe-req| probe-resp|reassoc]	Configures frame type to match from the list • all – Configures association frames • assoc – Authentication frames • auth – Beacon frames • beacon – Control frames • data – Data frames • deauth – Deauthentication frames • disassoc – Disassociation frames • mgmt – Management frames • probe-req – Probe request frames • probe-resp – Probe response frames • reassoc – Reassociation frames

Example

```
rfs7000-37FABE(config-test-signature-symbol)#frame-type reassoc
rfs7000-37FABE(config-test-signature-symbol)#
rfs7000-37FABE(config-test-signature-symbol)#frame-type all
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.5 mode

signature

Enables/Disables signature mode

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
mode enable
```

Parameters

mode enable	Enables/Disables signature mode

Example

```
rfs7000-37FABE(config-test-signature-symbol)#enable
rfs7000-37FABE(config-wips-policy-test)#
```

22.1.7.6 payload

signature

Configures the payload settings

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
payload  <1-3> pattern <WORD> offset <0-255>
```

Parameters

payload <1-3> pattern	Configures the payload settings • <1-3> pattern – Specify the payload index • <pattern> <WORD> – Specify the pattern to match hex or string • <WORD> – Specify the pattern name • offset <0-255> – Sets the offset in the payload to start the pattern match • <0-255> – Specify the offset value

Example

```
rfs7000-37FABE(config-test-signature-symbol)#payload 1 pattern symbol offset 1
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.7 src-mac

signature

Configures source MAC address

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
src-mac <MAC Address>
```

Parameters

src-mac <MAC Address>	Configures source MAC address • <MAC Address> – Specify the source MAC address to match

Example

```
rfs7000-37FABE(config-test-signature-symbol)#src-mac 00-1E-E5-EA-1D-60
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.8 ssid-match

signature

Configures the match based on SSID

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
ssid-match [ssid<WORD>|ssid-len <0-32> ]
```

Parameters

ssid-match [ssid|ssid-len]	Configures the match based on the SSID
	• ssid <WORD> – Specify the SSID string match
	  • <WORD> – Specify the SSID to match
	• ssid-len <0-32> – Specify the SSID length match
	  • <0-32> – Specify the SSID character length

Example

```
rfs7000-37FABE(config-test-signature-symbol)#ssid-match ssid dell
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.9 threshold-client

signature

Configures the wireless client threshold limit

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
threshold-client <0-65535>
```

Parameters

threshold-client <1-65535>	Configures the wireless client threshold limit • <1-65535> – Specify the threshold value for a 60 second window between 1 and 65535

Example

```
rfs7000-37FABE(config-test-signature-symbol)#threshold-client 88
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.10 threshold-radio

signature

Configures radio threshold limit

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
threshold-radio <1-65535>]
```

Parameters

threshold-radio <1-65535>	Configures the radio threshold limit • <1-65535> – Specify the threshold value for a 60 second window between 1 and 65535

Example

```
rfs7000-37FABE(config-test-signature-symbol)#threshold-radio 88
rfs7000-37FABE(config-test-signature-symbol)#
```

22.1.7.11 no

signature

Negates a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [bssid|dts-mac|filter-ageout|frame-type|mode|payload|src-mac|
ssid-match|threshold-client|threshold-radio]
```

Parameters

None

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs7000-37FABE(config-test-signature-signature1)#no bssid
rfs7000-37FABE(config-test-signature-signature1)#

rfs7000-37FABE(config-test-signature-signature1)#no dst-mac
rfs7000-37FABE(config-test-signature-signature1)#

rfs7000-37FABE(config-test-signature-signature1)#no filter-ageout
rfs7000-37FABE(config-test-signature-signature1)#

rfs7000-37FABE(config-test-signature-signature1)#no threshold-radio
rfs7000-37FABE(config-test-signature-signature1)#
```

CHAPTER 23 WLAN-QOS-POLICY

This chapter summarizes the WLAN QoS Policy in detail.

Use the (config) instance to configure WLAN QoS Policy related configuration commands. To navigate to the WLAN QoS Policy instance, use the following commands:

```
rfs7000-37FABE(config)#wlan-qos-policy <policyname>
rfs7000-37FABE(config)#wlan-qos-policy test
rfs7000-37FABE(config-wlan-qos-test)#?
WLAN QoS Mode commands:
accelerated-multicast  Configure accelerated multicast streams address and
                       forwarding QoS classification

classification        Select how traffic on this WLAN must be classified
                        (relative prioritization on the radio)
  multicast-mask       Configure egress prioritization multicast mask
                       (matching packets wont be queued up until DTIM)
  no                   Negate a command or set its defaults
  qos                  Quality of service
  rate-limit           Configure traffic rate-limiting parameters on a
                       per-wlan/per-client basis
  svp-prioritization   Enable spectralink voice protocol support on this wlan
  voice-prioritization Prioritize voice client over other client (for non-WMMclients)
  wmm                  Configure 802.11e/Wireless MultiMedia parameters

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs7000-37FABE(config-wlan-qos-test)#
```

23.1 wlan-qos-policy

Table 23.1 Summarizes WLAN QoS Policy commands

Table 23.1 *wlan-qos-policy Commands*

Command	Description	Reference
accelerated-multicast	Configures accelerated multicast streams address and forwards QoS classification	*page 23-3*
classification	Classifies the traffic on the WLAN based on priority	*page 23-4*
multicast-mask	Configures the egress prioritization multicast mask	*page 23-6*
no	Negates a command or sets its default values	*page 23-7*
qos	Defines the QoS configuration	*page 23-8*
rate-limit	Configures the traffic rate-limit on a WLAN using the WLAN QoS Policy.	*page 23-9*
svp-prioritization	Enables Spectralink voice protocol support on the WLAN	*page 23-11*
voice-prioritization	Prioritizes voice client over other clients	*page 23-12*
wmm	Configures 802.11e/wireless multimedia parameters	*page 23-13*

23.1.1 accelerated-multicast

wlan-qos-policy

Configures multicast streams for acceleration

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
accelerated-multicast [<A.B.C.D>|autodetect]
accelerated-multicast [<A.B.C.D>|autodetect] {classification} [background|best-effort|trust|video|voice]
```

Parameters

[<A.B.C.D>|autodetect] {classification} [background|best-effort|trust|video|voice]	• <A.B.C.D> – Configures the multicast address. It can be up to 32 IP addresses per wlan-qos-policy
	• autodetect – Allows the system to automatically detect multicast streams
	  • classification – Configures the forwarding QoS classification (traffic class)
	  • background – Forwards streams with background priority
	  • best-effort – Forwards streams with best effort priority
	  • trust – No change to the streams forwarding traffic class
	  • video – Forwards stream with video priority
	  • voice – Forwards stream with voice priority

Example

```
rfs7000-37FABE(config-wlan-qos-test)#accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

23.1.2 classification

wlan-qos-policy

Classifies traffic on the WLAN based on the priority

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
classification [low|normal|video|voice|wmm|non-unicast|non-wmm]
classification non-unicast [voice|video|normal|low|default]
classification non-wmm [voice|video|normal|low]
```

Parameters

[low|normal|video|voice|wmm|non-unicast]	• low – All the traffic on this WLAN is treated as low priority traffic (background) • normal – All the traffic on this WLAN is treated as normal priority (best effort) • video – All the traffic on this WLAN is treated as video • voice – All the traffic on this WLAN is treated as voice • wmm – Uses WMM based classification, using DSCP or 802.1p tags to classify traffic into different queues • non-wmm [voice|video|normal|low] – Selects the way, the traffic from non-WMM clients must be classified • non-unicast [voice|video|normal|low|default] – Configures the way broadcast and multicast traffic is classified • voice – Non-unicast traffic is classified and treated as voice packets • video – Non-unicast traffic is classified and treated as video packets • normal – Non-unicast traffic is classified and treated as normal priority packets (best effort) • low – Non-unicast traffic is classified and treated as low priority packets (background) • default – Uses the classification mode (same as unicast classification if WMM is disabled. Normal if unicast classification is WMM)

Example

```
rfs7000-37FABE(config-wlan-qos-test)#classification wmm
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#classification normal
rfs7000-37FABE(config-wlan-qos-test)#
```

```
rfs7000-37FABE(config-wlan-qos-test)#classification non-unicast voice
rfs7000-37FABE(config-wlan-qos-test)#
```

23.1.3 multicast-mask

wlan-qos-policy

Configure egress prioritization multicast mask

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
multicast-mask [primary|secondary] <WORD>
```

Parameters

[primary|secondary] <WORD>	Configures the primary and secondary egress prioritization multicast masks • <WORD> – Specifies the MAC address and mask in AA-BB-CC-DD-EE-FF/XX-XX-XX-XX-XX-XX format

Example

```
rfs7000-37FABE(config-wlan-qos-test)#multicast-mask primary 11-22-33-44-55-66/22-33-
44-55-66-77
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification normal
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 multicast-mask secondary 99-88-77-66-55-44/11-22-33-44-55-66
rfs7000-37FABE(config-wlan-qos-test)#
```

23.1.4 no

wlan-qos-policy

Negates a command or sets its default values

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
no [accelerated-multicast|classification|multicast-mask|qos|rate-limit|
svp-prioritization|voice-prioritization|wmm]
```

Parameters

[accelerated-multicast|classification|multicast-mask|qos|rate-limit|svp-prioritization|voice-prioritization|wmm]	• accelerated-multicast – Disables accelerated multicast streams address and forwarding QoS classification • classification – Removes the classification scheme • multicast-mask – Clears the egress prioritization multicast mask • qos – Quality of service • rate-limit – Disables the traffic rate-limiting parameters • svp-prioritization – Disables support for the Spectralink voice protocol on this WLAN • voice-prioritization – Disables the priority of voice clients over other clients (applies to non WMM clients) • wmm – Disables 802.11e/wireless multimedia parameters

Example

```
rfs7000-37FABE(config-wlan-qos-test)#no classification
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#no multicast-mask primary
rfs7000-37FABE(config-wlan-qos-test)#
rfs7000-37FABE(config-wlan-qos-test)#no qos trust dscp
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-unicast voice
 no qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs7000-37FABE(config-wlan-qos-test)#
```

23.1.5 qos

wlan-qos-policy

Enables quality of service

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
qos trust [dscp|wmm]
```

Parameters

trust [dscp|wmm]	Trust QOS values of ingressing packets • dscp – Trust IP DSCP values of ingressing packets • wmm – Trust 802.11 WMM QOS values of ingressing packets

Example

```
rfs7000-37FABE(config-wlan-qos-test)#qos trust wmm
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#qos trust dscp
rfs7000-37FABE(config-wlan-qos-test)#
```

23.1.6 rate-limit

wlan-qos-policy

Configures the WLAN traffic rate limit using the WLAN QoS policy

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
rate-limit [client|wlan] [from-air|to-air]
{[max-burst-size <2-1024>|rate <50-1000000>|
red-threshold [background|best-effort|video|voice]
 <0-100>]}
```

Parameters

[client|wlan] [from-air|to-air] {max-burst-size <2-1024>|rate <50-1000000> |red-threshold [background |best-effort|video| voice <0-100>]}	Configures the traffic rate-limit on a WLAN using this wlan-qos-policy. • client – Configures traffic rate limiting parameters on a per-client basis • wlan – Configures traffic rate limiting parameters on a per-wlan basis • from-air – Configures the traffic rate-limiting from a wireless client to the network • to-air – Configures the traffic rate limit from the network to a wireless client • max-burst-size <2-1024> – Sets the maximum burst size from 0-1024 • rate <50-1000000> – Sets the traffic rate in kbps from 50-1000000 • red-threshold – Configures the random early detection threshold for traffic class from the list • background <0-100> – Sets a threshold value for low priority traffic from 0-100 • best-effort <0-100> – Sets a threshold value for normal priority traffic from 0-100 • video <0-100> – Sets a threshold for video traffic from 0-100 • voice <0-100> – Sets a threshold for voice traffic from 0-100

Example

```
rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air max-burst-size 6
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air rate 55
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air red-threshold best-
effort 10
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#no rate-limit wlan from-air red-threshold best-
effort
rfs7000-37FABE(config-wlan-qos-test)#
rfs7000-37FABE(config-wlan-qos-test)#rate-limit client from-air red-threshold
background 3
rfs7000-37FABE(config-wlan-qos-test)#
rfs7000-37FABE(config-wlan-qos-test)#rate-limit client from-air rate 55
rfs7000-37FABE(config-wlan-qos-test)#
rfs7000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 voice-prioritization
 svp-prioritization
 wmm background cw-max 8
 wmm video txop-limit 9
 wmm voice cw-min 6
 wmm voice cw-max 6
 rate-limit client to-air max-burst-size 3
 rate-limit client from-air rate 55
 qos trust wmm
rfs7000-37FABE(config-wlan-qos-test)#
```

23.1.7 svp-prioritization

wlan-qos-policy

Enables WLAN Spectralink voice protocol support

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
svp-prioritization
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-qos-test)#svp-prioritization
rfs7000-37FABE(config-wlan-qos-test)#
```

23.1.8 voice-prioritization

wlan-qos-policy

Prioritizes voice client over other clients (for non-WMM clients)

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
voice-prioritization
```

Parameters

None

Example

```
rfs7000-37FABE(config-wlan-qos-test)#voice-prioritization
rfs7000-37FABE(config-wlan-qos-test)#
```

23.1.9 wmm

wlan-qos-policy

Configures 802.11e/wireless multimedia parameters

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP71xx
- AP650
- AP6511
- AP6532

Syntax

```
wmm [background|best-effort|power-save|qbss-load-element|video|voice]
wmm [background|best-effort||video|voice]
[aifsn <2-15>|cw-max <0-15>|cw-min <0-15>|txop-limit
<0-65535>]
```

Parameters

[background|best-effort|power- save|qbss-load-element|video|voice] [aifsn|cw-max|cw-mintxop-limit]	• background – Configures background access category parameters • best-effort – Configures best effort access category parameters • video – Configures video access category parameters • voice – Configure voice access category parameters The following parameters are common for all the above: • aifsn <2-15> – Configures the AIFSN: The wait time between data frames is derived from the AIFSN and slot time • <2-15> – Select a value between 1 and 15 to configure the AIFSN • cw-max <0-15> – Maximum contention window: Wireless clients pick a number between 0 and the min contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Sets a value from 0-15. • cw-min – Minimum contention window: Wireless clients pick a number between 0 and the min contention window to wait before re-transmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0-15. • txop-limit <0-65535> – Configures the transmit-opportunity: (the interval of time during which a particular client has the right to initiate transmissions) • <0-65535> – Select a value between 0 and 65535 to configure the transmit-opportunity in 32 microsecond units • power-save – Enables support for WMM-Powersave (U-APSD) • qbss-load-element – Enables support for the QBSS load information element in beacons and probe responses

Example

```
rfs7000-37FABE(config-wlan-qos-test)#wmm background aifsn 7
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#wmm video txop-limit 9
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#wmm voice cw-min 6
rfs7000-37FABE(config-wlan-qos-test)#

rfs7000-37FABE(config-wlan-qos-test)#wmm qbss-load-element
rfs7000-37FABE(config-wlan-qos-test)#
```

NOTE: clrscr, commit,end, exit, help, revert, service, show, write are common across all chapters. For more information, see *Chapter 5, COMMON COMMANDS*.

CHAPTER 24 INTERFACE-RADIO COMMANDS

Use the (config-profile-default-rfs4000) instance to configure radio instances associated with the controller.

To switch to this mode, use:

rfs4000-37FABE(config-profile-default-rfs4000)#interface radio ?

```
  1  Radio interface 1
  2  Radio interface 2
  3  Radio interface 3
rfs4000-37FABE(config-profile-default-rfs4000)#interface radio

rfs4000-37FABE(config-profile-default-rfs4000-if-radio1)#?
Radio Mode commands:
  aggregation             Configure 802.11n aggregation related parameters
  airtime-fairness        Enable fair access to medium for clients based on
                           their usage of airtime
  antenna-diversity        Transmit antenna diversity for non-11n rates

  antenna-gain             Specifies the antenna gain of this radio
  antenna-mode              Configure the antenna mode (number of transmit
and
                           receive antennas) on the radio
  beacon                   Configure beacon parameters
  channel                 Configure the channel of operation for this radio
  data-rates              Specify the 802.11 rates to be supported on this
                           radio
  description              Configure a description for this radio
  dynamic-chain-selection  Automatic antenna-mode selection (single
antenna
                            for non-11n transmit rates)
  guard-interval           Configure the 802.11n guard interval
  lock-rf-mode            Retain user configured rf-mode setting for this
                           radio
  max-clients              Maximum number of wireless clients allowed to
                           associate
  mesh                     Configure radio mesh parameters
  no                       Negate a command or set its defaults
  non-unicast              Configure handling of non-unicast frames
  off-channel-scan         Enable off-channel scanning on the radio
  placement                Configure the location where this radio is
                           operating
```

```
  power                          Configure the transmit power of the radio
  preamble-short                 User short preambles on this radio
  probe-response                 Configure transmission parameters for Probe
                                 Response frames
  radio-share-mode               Configure the radio-tap mode of operation for
this                                 radio
  rf-mode                      Configure the rf-mode of operation for this radio
                               rts-threshod
  rts-threshold                  Configure the RTS threshold
  shutdown                       Shutdown the selected radio interface
  sniffer-redirect               Capture packets and redirect to an IP address
                                 running a packet capture/analysis tool
  use                            Set setting to use
  wireless client                Configures wireless client related parameters
  wlan                           Enable wlans on this radio

  clrscr                         Clears the display screen
  commit                         Commit all changes made in this session
  do                             Run commands from Exec mode
  end                            End current mode and change to EXEC mode
  exit                           End current mode and down to previous mode
  help                           Description of the interactive help system
  revert                         Revert changes
  service                        Service Commands
  show                           Show running system information
  write                        Write running configuration to memory or terminal

rfs4000-37FABE(config-profile-default-rfs4000-if-radio1)#
```

24.1 interface-radio Instance

Table 24.1 Summarizes interface-radio commands

Table 24.1 *interface-radio commands*

Commands	Description	Reference
aggregation	Configures 802.11n aggregation related parameters	*page 24-5*
airtime-fairness	Enables fair access for clients based on their usage of airtime	*page 24-6*
antenna-diversity	Transmits antenna diversity for non-11n transmit rates	*page 24-7*
antenna-gain	Specifies the antenna gain of the selected radio	*page 24-8*
antenna-mode	Configures the antenna mode on the radio	*page 24-9*
beacon	Configures beacon parameters	*page 24-10*
channel	Configures the channel of operation for the radio	*page 24-11*
data-rates	Specifies the 802.11 rates supported on the radio	*page 24-12*
description	Configures a description for the selected radio	*page 24-15*
dynamic-chain-selection	Enables automatic antenna-mode selection	*page 24-16*
guard-interval	Configures the 802.11n guard interval	*page 24-17*
lock-rf-mode	Retains user configured rf-mode settings for the selected radio	*page 24-18*
max-clients	Defines the maximum number of wireless clients allowed to associate	*page 24-19*
mesh	Configures radio mesh parameters	*page 24-20*
no	Negates a command or sets its default value	*page 24-21*
non-unicast	Configures handling of non-unicast frames	*page 24-22*
off-channel-scan	Enables off-channel scanning on the radio	*page 24-23*
placement	Configures the location where the radio is in operation	*page 24-24*
power	Configures the transmit power on the radio	*page 24-25*
preamble-short	Configures user short preambles on the radio	*page 24-26*
probe-response	Configures transmission parameters for probe response frames	*page 24-27*
radio-share-mode	Configures the radio-tap mode for the radio	*page 24-28*
rf-mode	Configures the rf-mode for the radio	*page 24-29*
rifs	Configures *Reduced Interframe Spacing* (RIFS) parameters	*page 24-30*
rts-threshold	Configures RTS threshold value	*page 24-31*
shutdown	Terminates the selected radio interface	*page 24-32*
sniffer-redirect	Captures packets and redirects to an IP address running a packet capture/ analysis tool	*page 24-33*

Table 24.1 *interface-radio commands*

Commands	Description	Reference
use	TBD	*page 24-34*
wireless-client	Configures wireless client related parameters	*page 24-37*
wlan	Enables a WLAN on the radio	*page 24-35*

24.1.1 aggregation

interface-radio Instance

Configures 802.11n aggregation related parameters

Supported in the following platforms:

- RFS4011

Syntax

```
aggregation [ampdu|amsdu]
aggregartion ampdu [rx-only|tx-only|tx-rx|none|max-aggr-size|min-spacing]
aggregation ampdu max-aggr-size[rx|tx]
aggregation ampdu max-aggr-size rx [8191|16383|32767|65535
aggregation ampdu max-aggr-size tx [<0-65535>
aggregation amsdu [rx-only|tx-rx
aggregation ampdu min-spacing [0|1|2|4|8|16]]]
]
```

Parameters

ampdu [rx-only|tx-only| tx-rx|none|max-aggr-size| min-spacing]	ampdu – Configures *Aggregate MAC Protocol Data Unit* (A-MPDU) parameters
	• tx-only – Supports transmission of AMPDU parameters only
	• rx-only – Supports receiving of AMPDU parameters only
	• tx-rx – Supports both transmit as well as receiving of AMPDU parameters
	• none – Disables support for AMPDUs
	• max-aggr-size [rx|tx] – Configures limits on AMPDU packet sizes
	  • rx [8191|16383|32767|65535] – Sets the limit on received frames
	  • 8191– Advertises a maximum of 8191 bytes
	  • 16383 – Advertises a maximum of 16383 bytes
	  • 32767 – Advertises a maximum of 32767 bytes
	  • 65535 – Advertises a maximum of 65535 bytes
	  • tx [<0-65535>] – Sets the limit on transmitted frames
	  • <0-65535> – Set the limit in bytes
	• min-spacing – Configures the minimum gap between AMPDU frames

amsdu [rx-only|tx-rx]	amsdu – Configures *Aggregate MAC Service Data Unit* (A-MSDU) parameters • rx-only – Supports receiving of A-MSDU parameters only • tx-rx – Supports both transmit as well as receiving of A-MSDU parameters

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
aggregation ampdu tx-only
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
RFS4000-880DA7(config-profile-default-RFS4000-if-radio1)#show context
 interface radio1
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  aggregation ampdu tx-only
```

24.1.2 airtime-fairness

interface-radio Instance

Enables equal access for clients based on their usage of airtime

Supported in the following platforms:

- RFS4011

Syntax

```
airtime-fairness {prefer-ht} {weight <1-10>}
```

Parameters

{prefer-ht} {weight <1-10>}	• prefer-ht – Prefers high throughput (802.11n) clients over legacy clients> • weight <1-10> – Configures the relative weightage for 11n clients over legacy clients • <1-10> – Specify a weightage ratio for 11n clients between <1-10>

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
  airtime-fairness prefer-ht weight 6
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  aggregation ampdu tx-only
  airtime-fairness prefer-ht weight 6
```

24.1.3 antenna-diversity

interface-radio Instance

Transmits antenna diversity for non-11n transmit rates

Supported in the following platforms:

- RFS7000
- RFS6000
- RFS4000
- AP650
- AP71xx
- AP6511
- AP6532

Syntax

```
antenna-diversity
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-ap7131-if-radio1)#antenna-
diversity
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  aggregation ampdu tx-only
  airtime-fairness prefer-ht weight 6
  antenna-diversity
```

24.1.4 antenna-gain

interface-radio Instance

Specifies the antenna gain of the selected radio

Supported in the following platforms:

- RFS4011

Syntax

```
antenna-gain <0.0-15.0>
```

Parameters

<0.0-15.0>	Select the antenna gain in units of dBi between <0.0-15.0>

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#antenna-gain
12.0
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.5 antenna-mode

interface-radio Instance

Configures the antenna mode on the radio

Supported in the following platforms:

- RFS4011

Syntax

```
antenna-mode [1*1|1*3|2*2|default]
```

Parameters

[1*1|1*3|2*2|default]	• 1x1 – Uses only antenna A to receive and transmit • 1x3 – Uses antenna A to transmit, and receives on other antennas • 2x2 – Uses antenna A and C for both transmit and receive • default – Uses default antenna settings

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
  antenna-mode 2x2
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.6 beacon

interface-radio Instance

Configures beacon parameters

Supported in the following platforms:

- RFS4011

Syntax

```
beacon [dtim-period|period]
beacon dtim-period [<1-50>|bss <1-8> <1-50>]]
beacon period [50|100|200]
```

Parameters

dtim-period	Configures the dtim interval used on the radio
	• <1-50> – Specify a single value used on the radio
	• bss <1-8> <1-50> – Specify a separate dtim value for bss on the radio
	  • <1-8> – Specify the bss number between <1-8>
	  • <1-50> – Specify the dtim value used on a selected bss

period [50|100|200]	Configures the beacon interval • 50 – 50 K-uSec interval between beacons • 100 – 100 K-uSec interval between beacons (default) • 200 – 200 K-uSec interval between beacons

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#beacon dtim-
period bss 2 20
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#beacon period 50
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.7 channel

interface-radio Instance

Configures the channel of operation on the radio

Supported in the following platforms:

- RFS4011

Syntax

```
channel [smart|12|3|4|-------]
```

Parameters

smart|12|3|4|-------]	• smart – Uses Smart RF to assign a channel (uses uniform spectrum spreading if Smart RF is not enabled) • 1 – Channel 1 in 20Mhz • 2 – Channel 1 in 20Mhz

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#channel 1
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  channel 1
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#channel smart
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.8 data-rates

interface-radio Instance

Specifies the 802.11 rates supported on the radio

Supported in the following platforms:

- RFS4011

Syntax

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default|custom
data-rates custom [1|2|5.5|6|9|11|12|18|24|36|48|54| mcs0-7|mcs8-15|
mcs0-15|basic-1|basic-2| basic-5.5|basic-6|basic-9| basic-11|basic-12|
basic-18|basic-24|basic-36|basic-48|basic-54|basic-mcs0-7]]
```

Parameters

b-only	Supports operation in 11b-only mode
g-only	Uses rates that support operation in 11g-only mode
a-only	Uses rates that support operation in 11a-only mode
bg	Uses rates that support both 11b and 11g clients
bgn	Uses rates that support 11b, 11g and 11n clients
gn	Uses rates that support 11g and 11n clients
an	Uses rates that support 11a and 11n clients

default	Enables the default data-rates according to the band of operation of the radio
custom	Configures a list of data rates by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it is to be used as a basic rate (Eg: 'data-rates custom basic-1 basic-2 5.5 11') • 1 – 1-Mbps • 2 – 2-Mbps • 5.5 – 5.5-Mbps • 6 – 6-Mbps • 9 – 9-Mbps • 11– 11-Mbps • 12 – 12-Mbps • 18 –18-Mbps • 24 – 24-Mbps • 36 – 36-Mbps • 48 – 48-Mbps • 54 – 54-Mbps • mcs0-7 – Modulation and Coding Scheme 0-7 • mcs8-15 – Modulation and Coding Scheme 8-15 • mcs0-15 – Modulation and Coding Scheme 0-15 • basic-1 – Basic 1-Mbps • basic-2 – Basic 2-Mbps • basic-5.5 – Basic 5.5-Mbps • basic-6 – Basic 6-Mbps • basic-9 – Basic 9-Mbps • basic-11 – Basic 11-Mbps • basic-12 – Basic 12-Mbps • basic-18 – Basic 18-Mbps • basic-24 – Basic 24-Mbps • basic-36 – Basic 36-Mbps • basic-48 – Basic 48-Mbps • basic-54 – Basic 54-Mbps • basic-mcs0-7 – Modulation and Coding Scheme 0-7 as a basic rate

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#data-rates b-
only
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  data-rates b-only
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#data-rates
custom basic-mcs0-7
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  data-rates custom basic-mcs0-7
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.9 description

interface-radio Instance

Configures a description for the selected radio

Supported in the following platforms:

- RFS4011

Syntax

```
description <WORD>
```

Parameters

<WORD>	Configures a description for the selected radio

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#description
radio1
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.10 dynamic-chain-selection

interface-radio Instance

Enables automatic antenna-mode selection (single antenna for non-11n transmit rates)

Supported in the following platforms:

- RFS4011

Syntax

```
dynamic-chain-selection
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#dynamic-chain-
selection
RFS4000-880DA7(config-profile-default-RFS4000-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.11 guard-interval

interface-radio Instance

Configures the 802.11n guard interval. Guard intervals are used to ensure that distinct transmissions do not interfere with one another. Its is used to provide immunity to propagation delays, echoes and reflection of radio signal.

Supported in the following platforms:

- RFS4011

Syntax

```
guard-interval [any|long]
```

Parameters

any	Allows the radio to use any short (400nSec) or long (800nSec) guard interval
long	Specify the use of long guard interval (800nSec)

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#guard-interval
long
RFS4000-880DA7(config-profile-default-RFS4000-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.12 lock-rf-mode

interface-radio Instance

Retains user configured rf-mode settings for the selected radio through reboots.

Supported in the following platforms:

- RFS4011

Syntax

```
lock-rf-mode
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#lock-rf-mode
RFS4000-880DA7(config-profile-default-RFS4000-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.13 max-clients

interface-radio Instance

Defines the maximum number of wireless clients allowed to associate

Supported in the following platforms:

- RFS4011

Syntax

```
max-clients <0-256>
```

Parameters

<0-256>	Specify the maximum number of clients allowed to associate with the radio

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#max-clients 100
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
RFS4000-880DA7(config-profile-default-RFS4000-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
```

24.1.14 mesh

interface-radio Instance

Configures radio mesh parameters

Supported in the following platforms:

- RFS4011

Syntax

```
mesh [client|links <1-6>|portal|preferred-peer <1-6> <MAC>]
```

Parameters

[client|links <1-6> |portal|preferred-peer <1-6> <MAC>]	• client – Enables operation as a client. (Scan for mesh portals, or nodes that have connectivity to portals, and connect through them)
	• links <1-6> – Configures the maximum number of mesh links that the radio will attempt to create
	  • <1-6> – Specify the maximum number of mesh links from the radio
	• portal – Enables operation as a portal. (Begins beaconing immediately, accepting connections from other mesh nodes. Typically the node with a connection to the wired network)
	• preferred-peer <1-6> <MAC> – Configures a peer device to which connection should be preferred
	  • <1-6> – Configures the priority at which the peer node will be added
	  • <MAC> – Specify the MAC address of the preferred peer device (Ethernet MAC of either an AP or a controller with onboard radios)

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#mesh preferred-
peer 2 11-22-33-44-55-66
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#mesh client
RFS4000-880DA7(config-profile-default-RFS4000-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  mesh client
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  airtime-fairness prefer-ht weight 6
```

24.1.15 no

interface-radio Instance

Negates a command or sets its default value

Supported in the following platforms:

- RFS4011

Syntax

```
no <parameter>
```

Parameters

None

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no aggregation
ampdu max-aggr-size  rx
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no mesh links
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#no rifs mode
```

24.1.16 non-unicast

interface-radio Instance

Configures handling of non-unicast frames

Supported in the following platforms:

- RFS4011

Syntax

```
non-unicast [forwarding|queue|tx-rate]
non-unicast forwarding [follow-dtim|power-save-aware]
non-unicast queue [<1-200>|bss <1-8> <1-200>]
non-unicast tx-rate [bss <1-8>|dynamic-all|dynamic-basic|highest-
basic|lowest-basic]
non-unicast tx-rate bss <1-8> {dynamic-all|dynamic-basic|highest-basic|
lowest-basic}
```

Parameters

forwarding [follow-dtim| power-save-aware]	Configures the method by which multicast and broadcast frames are forwarded by the radio • follow-dtim – Specifies the frames always wait for the DTIM interval • power-save-aware – If all associated wireless-clients are in a power-save active mode, then the frames are forwarded immediately

queue [<1-200>|bss <1-8> <1-200>]	Configures the number of broadcast packets that are queued up per bss on the radio
	• <1-200> – Specify the number of packets per bss
	• bss <1-8> <1-200> – Overrides the default on a specific bss number
	  • <1-8> <1-200> – Specify the bss number
	  • <1-200> – Specifies the number of packets queued

tx-rate [bss <1-8>| dynamic-all|dynamic-basic| highest-basic|lowest-basic]	Configures the data-rate at which broadcast and multicast frames will be transmitted • bss <1-8> {dynamic-all|dynamic-basic|highest-basic| lowest-basic} – Overrides the default on a specific bss number • <1-8> – Specify the bss number • dynamic-all –Select a rate among all the supported rates based on current traffic conditions • dynamic-basic – Select a rate among all the basic rates based on current traffic conditions • highest-basic – Uses the highest configured basic rate on the radio • lowest-basic – Uses the lowest configured basic rate on the radio

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#non-unicast
queue bss 2 3
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#non-unicast tx-
rate bss 1 dynamic-all
```

24.1.17 off-channel-scan

interface-radio Instance

Enables off channel scanning on the radio

Supported in the following platforms:

- RFS4011

Syntax

`off-channel-scan {channel-list [2.4Ghz {<WORD>}|5Ghz {<WORD>}]|sniffer-redirect <A.B.C.D>}`

Parameters

channel-list [2.4Ghz {<WORD>}|5Ghz {<WORD>}]	channel-list [2.4GHz {<WORD>}|5GHz {<WORD>} – Specifies the channel list to scan • 2.4GHz <WORD> – 2.4GHz band • 5GHz <WORD> – 5GHz band • <WORD> – Specify a list of 20MHz/40MHz channels
sniffer-redirect <A.B.C.D>	Captures packets and redirects to an IP address running a packet capture analysis tool • <A.B.C.D> – Specify the IP address of the destination device

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#off-channel-
scan channel-list 2.4GHz 1
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#off-channel-
scan channel-list 5GHz
wm3400-229D58(config-profile-default-wm3400-if-radio1)#off-channel-scan
channel-list 2.4GHz 1,2
wm3400-229D58(config-profile-default-wm3400-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  mesh client
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  off-channel-scan channel-list 2.4GHz 1,2
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
```

24.1.18 placement

interface-radio Instance

Configures the location where the radio is in operation

Supported in the following platforms:

- RFS4011

Syntax

```
placement [indoor|outdoor]
```

Parameters

[indoor|outdoor]	• indoor – Radio is deployed indoors (uses indoor regulatory rules) • outdoor – Radio is deployed outdoors (uses outdoor regulatory rules)

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#placement
outdoor
wm3400-229D58(config-profile-default-wm3400-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  placement outdoors
  mesh client
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  off-channel-scan channel-list 2.4GHz 1,2
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
```

24.1.19 power

interface-radio Instance

Configures the transmit power on the radio

Supported in the following platforms:

- RFS4011

Syntax

```
power [<1-27>|smart]
```

Parameters

[<1-27>|smart]	• <1-27> – Transmits power in dBm (actual power could be lower based on regulatory restrictions) • smart – Smart RF decides optimum power required

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#power 12
wm3400-229D58(config-profile-default-wm3400-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  power 12
  data-rates custom basic-mcs0-7
  mesh client
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  off-channel-scan channel-list 2.4GHz 1,2
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
```

24.1.20 preamble-short

interface-radio Instance

Configures short preamble on the radio

Supported in the following platforms:

- RFS4011

Syntax

```
preamble-short
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#preamble-short
wm3400-229D58(config-profile-default-wm3400-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  mesh client
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  off-channel-scan channel-list 2.4GHz 1,2
  preamble short
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
```

24.1.21 probe-response

interface-radio Instance

Configures transmission parameters for probe response frames

Supported in the following platforms:

- RFS4011

Syntax

```
probe-response [rate|retry]
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

Parameters

rate [follow-probe-request| highest-basic|lowest-basic]	Configures the data rates at which the probe responses are transmitted • follow-probe-request – Transmits probe responses at the same rate the request was received • highest-basic – Uses the highest configured basic rate of the radio • lowest-basic – Uses the lowest configured basic rate of the radio
retry	Retransmits probe response if no acknowledgement is received from the client

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#probe-response
retry
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#probe-response
rate highest-basic
```

24.1.22 radio-share-mode

interface-radio Instance

Configures the radio-share mode of operation for this radio

Supported in the following platforms:

- RFS4011

Syntax

```
radio-share-mode [inline|off|promiscuous]
```

Parameters

[inline|off|promiscuous]	• inline – Enables sharing of all wlan packets serviced by this radio (matching the bssid of the radio) • off – Disables radio-share (no packets shared with wips sensor module) • promiscuous – Enables sharing of all packets that the radio can receive in promiscuous mode without filtering based on its bssid

Example

```
rfs4000-37FABE(config-profile-default-ap7131-if-radio1)#radio-share-mode
promiscuous
wm3400-229D58(config-profile-default-wm3400-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  mesh client
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  off-channel-scan channel-list 2.4GHz 1,2
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  max-clients 100
  radio-share-mode promiscuous
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
```

24.1.23 rf-mode

interface-radio Instance

Configures the rf-mode for the radio

Supported in the following platforms:

- RFS4011

Syntax

```
rf-mode [2.4GHz-wlan|5GHz-wlan|sensor]
```

Parameters

2.4GHz|5GHz|sensor]	• 2.4GHz-wlan – Provides WLAN service in 2.4GHz band • 5GHz-wlan – Provides WLAN service in 5GHz band • sensor – Operates as a sensor radio

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#rf-mode sensor
wm3400-229D58(config-profile-default-wm3400-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  rf-mode sensor
  data-rates custom basic-mcs0-7
  mesh client
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  off-channel-scan channel-list 2.4GHz 1,2
  guard-interval long
  aggregation ampdu tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
```

24.1.24 rifs

interface-radio Instance

Configures *Reduced Interframe Spacing* (RIFS) parameters

Supported in the following platforms:

- RFS4011

Syntax

```
rifs [none|rx-only|tx-only|tx-rx]
```

Parameters

[none|rx-only|tx-only|tx-rx]	• none – Disables support for RIFS • rx-only – Supports RIFS possession only • tx-only – Support RIFS transmission only • tx-rx– Supports both RIFS transmission and possession

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#rifs tx-only
wm3400-229D58(config-profile-default-wm3400-if-radio1)#show context
 interface radio1
  description Primary\ Radio
  data-rates custom basic-mcs0-7
  mesh client
  wlan 1 bss 1 primary
  wlan wlan1 bss 1
  antenna-gain 12.0
  off-channel-scan channel-list 2.4GHz 1,2
  guard-interval long
  aggregation ampdu tx-only
  rif tx-only
  antenna-mode 2x2
  dynamic-chain-selection
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
```

24.1.25 rts-threshold

interface-radio Instance

Configures RTS threshold value

Supported in the following platforms:

- RFS4011

Syntax

```
rts-threshold <0-2347>
```

Parameters

<0-2347>	Specify RTS threshold in bytes between <0-2347>

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#rts-threshold
10
```

24.1.26 shutdown

interface-radio Instance

Terminates the selected radio interface

Supported in the following platforms:

- RFS4011

Syntax

```
shutdown
```

Parameters

None

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#shutdown
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

24.1.27 sniffer-redirect

interface-radio Instance

Captures packets and redirects to an IP address running a packet capture/analysis tool

Supported in the following platforms:

- RFS4011

Syntax

```
sniffer-redirect <A.B.C.D> channel [1|1+|10|10---------165
```

Parameters

<A.B.C.D> channel [1|1+|10|10---------165]	<A.B.C.D> – Specify the IP address of the destination device
	• channel [1|1+|10|10---------165 – Specify the channel to capture packets
	  • 1 – Channel 1 in 20Mhz
	  • 1+ – Channel 1 as primary, Channel 5 as extension
	  • 10 – Channel 10 in 20Mhz

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#sniffer-
redirect 172.16.10.13 channel ?
  1     Channel 1 in 20Mhz
  1+    Channel 1 as primary, Channel 5 as extension
  10    Channel 10 in 20Mhz
  10-   Channel 10 as primary, Channel 6 as extension
  100   Channel 100 in 20Mhz
------------------------------------------------------------------------
------------------------------------------------------------------------
--
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

24.1.28 use

interface-radio Instance

The use command is used to apply other configuration profiles or values on to the current configuration item. In this case, association acl policy and radio-qos-policy can be used by this radio interface.

Supported in the following platforms:

- RFS4011

Syntax

```
use [association-acl-policy <ASSOC-ACL>|radio-qos-policy <RADIO-QOS>]
```

Parameters

[association-acl-policy <ASSOC-ACL>|radio-qos-policy <RADIO-QOS>]	• [association-acl-policy <ASSOC-ACL> – Specify the name of the association-acl-policy used • radio-qos-policy <RADIO-QOS> – Specify the name of the radio-qos-policy used

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#use
association-acl-policy test
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

24.1.29 wlan

interface-radio Instance

Enables WLAN on the radio

Supported in the following platforms:

- RFS4011

Syntax

```
wlan <WLAN> {bss|primary}
wlan <WLAN> bss <1-8> {primary}
```

Parameters

<WLAN> {bss <1-8> |primary}	<WLAN> {bss <1-8> |primary} – Specify the name of the WLAN (it must have been already created and configured) • bss <1-8> {primary} – Optional. Provide a specific bss number on the radio where the selected WLAN has to be mapped • <1-8> – Specify the bss number • primary – Optional. Pretends the selected WLAN as the primary WLAN if there are multiple WLANs on its bss

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#wlan wlan1
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#

rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 3
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  rts-threshold 10
  wlan wlan1 bss 1 primary
  off-channel-scan channel-list 5GHz
  off-channel-scan channel-list 2.4GHz 1
  off-channel-scan sniffer-redirect 172.16.10.100
  rifs tx-rx
  use association-acl-policy test
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast queue bss 1 2
  non-unicast queue bss 2 1
  non-unicast queue bss 3 1
  non-unicast queue bss 4 1
  non-unicast queue bss 5 1
```

```
  non-unicast queue bss 6 1
  non-unicast queue bss 7 1
  non-unicast queue bss 8 1
  probe-response rate highest-basic
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

24.1.30 wireless-client

interface-radio Instance

Configures wireless client related parameters

Supported in the following platforms:

- RFS4011

Syntax

```
wireless-client tx-power <0-20>
```

Parameters

tx-power <0-20>	Configures the transmit power indicated to wireless clients • <0-20> – Specify transmit power between 0 and 20 dBm

Example

```
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#wireless-client
tx-power 2
rfs4000-880DA7(config-profile-default-rfs4000-if-radio1)#
```

CHAPTER 25 FIREWALL LOGGING

This chapter summarizes the Firewall Logging commands within the CLI.

The firewall uses logging to send system messages to one or more logging destinations, where they can be collected, archived and reviewed.

Set the logging level to define which messages are sent to each of the target destinations.

Logging messages can be sent to any of the following destinations:

- The firewall console
- Telnet or SSH sessions to the firewall
- A temporary buffer internal to the firewall
- Syslog servers
- E-mail addresses
- An FTP server

25.1 Firewall Log Terminology and Syslog Severity Levels

Abbreviation	*Description*
FTP	File transfer protocol
ACL	Access control list
Src MAC	Source MAC address
Dest MAC	Destination MAC address
LOGRULEHIT	ACL rule applied
PKT DROP	Packet drop
Src IP	Source IP address
Dest IP / Dst IP	Destination IP address
FWSTARTUP	Firewall enabled
DP	Destination port
SP	Source port
Matched Temporary Rule	This is a internal rule created to allow data traffic for ALG like TFTP, FTP, HTTPs and so on

Syslog Severity Level as Message	**Severity Level as Numeric**	**Description**
emergency	0	System is unusable
alert	1	Immediate action needed
critical	2	Critical condition
error	3	Error condition
warning	4	Warning condition
notification	5	Normal but significant condition
informational	6	Informational message
debugging	7	Debugging message

25.1.1 Date format in Syslog messages

The following output displays date in proper format

```
rfs7000-81916A(config)#May 19 16:20:00 2010: USER: cfgd: deleting session 4
rfs7000-81916A(config)#
rfs7000-81916A(config)#May 19 16:20:17 2010: USER: cfgd: deleting session 5
```

The date format is Month <MMM> Date <DD> Time <HH:MM:SS> Year <YYYY>

Month is May

Date is 19

Time is 16:20:00

Year is 2010

To generate a date log, enable logging

For example, the following command has to be executed.

```
rfs7000-37FABE#clock set 16:20:00 19 May 2010
rfs7000-37FABE#
```

25.1.2 FTP data connection log

To generate a FTP data connection log, an ACL rule has to be applied and logging has to be enabled.

The FTP connection is Control Connection

May 19 16:31:19 2010:%DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.2.102 Proto:6 Src Port:3014 Dst Port:21

Date is May19

Time is 16:31:19

Year is 2010

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is LOGRULEHIT

Log Message is Matched ACL

The Matching ACL is FTPuser

ip Rule sequence number is 0

Disposition is Allow Packet

Source MAC Address is 00-19-B9-6B-DA-77

Destination MAC Address is <00-15-70-81-91-6A>

Ethertype is 0x0800

Source IP Address is 192.168.1.99

Destination IP Address is 192.168.2.102

Protocol Type is 6

Source Port is 3014D

Destination Port is 21

NOTE: The same terminology is used across all logs.

The Data Connection in Active Mode

May 19 16:35:54 2010: %DATAPLANE-5-LOGRULEHIT: Matched Temporary Rule of FTP ALG. Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.1.99 Proto:6 Src Port:20 Dst Port:3017.

The Data Connection in Passive Mode

May 19 17:14:31 2010: %DATAPLANE-5-LOGRULEHIT: Matched Temporary Rule of FTP ALG. Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.2.102 Proto:6 Src Port:3033 Dst Port:3894.

For example,

```
rfs7000-37FABE(config-mac-acl-test)#permit any any log rule-precedence 25
rfs7000-37FABE(config-mac-acl-test)#
```

25.1.3 UDP packets log

In both DHCP release and DHCP renew scenarios, the destination port 67 is logged.

DHCP Release

May 19 18:57:43 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:172.16.31.196 Proto:17 Src Port:68 Dst Port:67.

DHCP Renew

May 19 18:58:48 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<FF-FF-FF-FF-FF-FF> Ethertype:0x0800 Src IP:0.0.0.0 Dst IP:255.255.255.255 Proto:17 Src Port:68 Dst Port:67.

To generate a UDP packet log, an ACL rule has to be applied to UDP packets and logging has to be enabled.

For example,

```
rfs7000-37FABE(config-ip-acl-test)#permit udp any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

25.1.4 ICMP type logs

The example below displays an ICMP Type as 13 and an ICMP Code as 0.

May 19 19:12:13 2010:%DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.1.103 Proto:1 ICMP Type:13 ICMP Code:0.

The below example displays an ICMP Type as 15 and an ICMP Code as 0.

May 20 10:35:49 2010:%DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Allow Packet Src MAC:<00-60-80-B0-C3-B3> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.104 Dst IP:192.168.2.102 Proto:1 ICMP Type:15 ICMP Code:0.

The below example displays an ICMP Type as 17 and an ICMP Code as 0.

May 19 19:26:18 2010:%DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.1.103 Proto:1 ICMP Type:17 ICMP Code:0.

The below example displays an ICMP Type as 18 and an ICMP Code as 0.

May 20 10:28:24 2010:%DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 18. Reason: no flow matching payload of ICMP Reply.

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is ICMPPKTDROP

Log Message is Dropping ICMP Packet

To generate an ICMP log, an ACL rule has to be applied on ICMP packets, and logging has to be enabled.

For example, the following commands have to be executed.

```
rfs7000-37FABE(config-ip-acl-test)#permit icmp any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

25.1.5 ICMP type logs

The following example displays an ICMP Type as 3 and a Code as 3.

May 19 19:56:00 2010:%DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP type 3. Reason: no flow matching payload of ICMP Error.

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is ICMPPKTDROP

Log Message is Dropping ICMP Packet

The following example displays an ICMP Type as 4 and a Code as 0.

May 19 21:13:36 2010:%DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 4. Reason: ICMP dest IP does not match inner source IP.

The following example displays an ICMP Type as 5 and a Code as 0.

May 19 21:15:12 2010:%DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 5. Reason: ICMP dest IP does not match inner source IP.

The following example displays an ICMP type as 11 and a Code as 0.

May 20 10:24:52 2010:%DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.2.102 to 192.168.1.103, with ProtocolNumber:1 ICMP code 0 and ICMP type 11. Reason: ICMP dest IP does not match inner source IP.

The following example displays an ICMP type as 14 and a Code as 0.

May 20 10:33:57 2010:%DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 14. Reason: no flow matching payload of ICMP Reply.

The following example displays an ICMP type as 16 and a Code as 0.

May 20 10:37:11 2010:%DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP type 16. Reason: no flow matching payload of ICMP Reply.

To generate an ICMP log, logging has to be enabled.

For example, the following commands has to be executed.

```
rfs7000-37FABE(config-fw-policy-default)#logging icmp-packet-drop all
rfs7000-37FABE(config-fw-policy-default)#
```

25.1.6 Raw IP Protocol logs

The following example displays a TCP header length as less than 20 bytes:

May 19 20:02:50 2010: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header length less than 20 bytes : Src IP : 192.168.2.102, Dst IP: 192.168.1.104, Src Mac: 00-11-25-14-D9-E2, Dst Mac: 00-15-70-81-91-6A, Proto = 6..

Module name is DATAPLANE

Syslog Severity level is 4

Log ID is DOSATTACK

Log Message is INVALID PACKET

May 19 20:02:50 2010: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from 192.168.2.102 to 192.168.1.104 Protocol Number: 6. Reason: malformed TCP header.

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is MALFORMEDIP

Log Message is Dropping IPv4Packet

To generate a raw IP protocol log, logging has to be enabled.

For example, the following commands has to be executed.

```
rfs7000-37FABE(config-fw-policy-default)# logging verbose
rfs7000-37FABE(config-fw-policy-default)#
rfs7000-37FABE(config-fw-policy-default)# logging malformed-packet-drop all
rfs7000-37FABE(config-fw-policy-default)#
```

When logging verbose is enabled, the log is displayed as:

Aug 18 15:57:21 2010: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from 192.168.0.91 to 192.168.0.1 Protocol Number: 6 SrcPort: 22616 DstPort: 22616 Reason: no matching TCP flow.

Module name is DATAPLANE

Syslog Severity level is 5

Log ID is MALFORMEDIP

Log Message is Dropping IPv4Packet

25.1.7 Raw IP Protocol logs

The following example displays TCP without data:

May 19 20:02:50 2010: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header length less than 20 bytes : Src IP : 192.168.2.102, Dst IP: 192.168.1.104, Src Mac: 00-11-25-14-D9-E2, Dst Mac: 00-15-70-81-91-6A, Proto = 6.

May 19 20:02:50 2010: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from 192.168.2.102 to 192.168.1.104 Protocol Number: 6. Reason: malformed TCP header.

To generate a raw ip protocol log, logging has to be enabled.

For example, the following commands has to be executed.

```
rfs7000-37FABE(config-fw-policy-default)# logging verbose
rfs7000-37FABE(config-fw-policy-default)#
rfs7000-37FABE(config-fw-policy-default)# logging rawip-packet-drop all
rfs7000-37FABE(config-fw-policy-default)#
```

When logging verbose is enabled, the log is displayed as:

Aug 18 15:57:49 2010: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header length less than 20 byt es : Src IP : 192.168.0.91, Dst IP: 192.168.0.1, Src Mac: 00-16-36-05-72-2A, Dst Mac: 00-23-68-22-C8-6E, Proto = 6.

Aug 18 15:57:49 2010: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from 192.168.0.91 to 192.168.0.1 Protocol Number: 6 . Reason: malformed TCP header.

Module name is DATAPLANE

Syslog Severity level is 4

Log ID is DOSATTACK

Log Message is INVALID PACKET

25.1.8 Firewall startup log

The following example displays an enabled firewall. A firewall enabled message is displayed in **bold**.

System bootup time (via /proc/uptime) was 93.42 42.52

Please press Enter to activate this console. May 19 20:10:09 2010: %NSM-4-IFUP: Interface vlan2 is up

May 19 20:10:09 2010: KERN: vlan2: add 01:00:5e:00:00:01 mcast address to master interface.

May 19 20:10:09 2010: %NSM-4-IFUP: Interface vlan172 is up

May 19 20:10:09 2010: KERN: vlan172: add 01:00:5e:00:00:01 mcast address to master interface.

May 19 20:10:09 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/lighttpd"

May 19 20:10:09 2010: %FILEMGMT-5-HTTPSTART: lighttpd started in external mode with pid 0

May 19 20:10:09 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

May 19 20:10:09 2010: %USER-5-NOTICE: FILEMGMT[1086]: FTP: ftp server stopped

May 19 20:10:09 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

May 19 20:10:10 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

May 19 20:10:10 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan2

May 19 20:10:10 2010: %DOT11-5-COUNTRY_CODE: Country of operation configured to in [India]

May 19 20:10:10 2010: %DIAG-6-NEW_LED_STATE: LED state message AP_LEDS_ON from module DOT11

May 19 20:10:10 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/telnetd"

May 19 20:10:10 2010: %AUTH-6-INFO: sshd[1422]: Server listening on 0.0.0.0 port 22.

dataplane enabled

CCB:21:Firewall enabled

May 19 20:10:11 2010: %KERN-4-WARNING: dataplane enabled.

May 19 20:10:11 2010: %DATAPLANE-5-FWSTARTUP: **Firewall enabled.**

May 19 20:10:13 2010: USER: cfgd: handle_cluster_member_update

May 19 20:10:13 2010: USER: cfgd: ignoring, no cluster configured

May 19 20:10:13 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/sshd"

25.1.9 Manual time change log

The following example displays the manual time changes log. The clock is manually set to May 19 18:49:07 2010.

Log change in time

rfs7000-81916A#show clock

May 19 14:39:11 UTC 2010

rfs7000-81916A#clock set 18:49:00 19 May 2010

May 19 14:39:18 2010: %[S1]CFGD-6-SYSTEM_CLOCK_RESET: System clock reset, Time: 2010-05-19 18:49:00[S2]

rfs7000-81916A#show clock

May 19 18:49:07 UTC 2010

rfs7000-81916A#

To generate a time log, logging has to be enabled

For example, the following command has to be executed:

```
rfs7000-37FABE#clock set 18:49:07  19 May 2010
rfs7000-37FABE#
```

25.1.10 Firewall ruleset log

The following example displays the log changes as ' ACL_ATTACHED_ALTERED' when an ACL Rule is applied/removed on WLAN, VLAN, GE, and PORT-CHANNEL.

IP ACL IN on WLAN Attach

May 21 12:48:40 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered

USER: The user who is doing the change

session: means the session id of the user - one user can have multiple sessions running, so this explains from which session this change was done

ACL : Name of the ACL that has rules added/deleted

IP ACL IN on WLAN Remove

May 21 12:49:26 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

IP ACL OUT on WLAN Attach

May 21 12:52:49 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

IP ACL OUT on WLAN Remove

May 21 12:52:58 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

MAC ACL IN on WLAN Attach

May 21 12:54:25 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

MAC ACL IN on WLAN Remove

May 21 12:54:32 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

MAC ACL OUT on WLAN Attach

May 21 12:56:29 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

MAC ACL OUT on WLAN Remove

May 21 12:56:37 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

IP ACL on VLAN Attach

May 21 12:58:44 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface vlan1 is getting altered.

IP ACL on VLAN Remove

May 21 12:59:30 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface vlan1 is getting altered.

IP ACL on GE Port Attach

May 21 13:01:41 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

IP ACL on GE Port Remove

May 21 13:01:25 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

MAC ACL on GE Port Attach

May 21 13:03:15 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

MAC ACL on GE Port Remove

May 21 13:06:19 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

IP ACL on Port-Channel Attach

May 21 13:07:12 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface port-channel1 is getting altered.

IP ACL on Port-Channel Remove

May 21 13:07:26 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface port-channel1 is getting altered.

MAC ACL on Port-Channel Attach

May 21 13:09:13 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface port-channel1 is getting altered.

MAC ACL on Port-Channel Remove

May 21 13:09:24 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL attached to interface port-channel1 is getting altered.

Rule added / deleted from IP/MAC ACL

Feb 26 20:32:56 2010: %CFGD-6-ACL_RULE_ALTERED: USER: admin session 3: ACL foo rule is getting altered.

25.1.11 TCP Reset Packets log

For any change in the TCP configuration, a TCP reset log is generated. The following example displays the initial TCP packets permitted before the session timedout.

May 19 20:31:26 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.2.102 Proto:6 Src Port:3318 Dst Port:21.

May 19 20:31:31 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.2.102 Proto:6 Src Port:3318 Dst Port:21.

25.1.12 ICMP Destination log

The following example displays an ICMP destination is unreachable when no matching payload is found.

May 19 19:57:09 2010: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP type 3. Reason: no flow matching payload of ICMP Error.

May 19 19:57:09 2010: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP type 3. Reason: no flow matching payload of ICMP Error.

To generate an ICMP protocol log, an ACL rule has to be applied and logging has to be enabled.

For example, the following commands has to be executed.

```
rfs7000-37FABE(config-ip-acl-test)#permit icmp any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

25.1.13 ICMP Packet log

May 19 20:37:04 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Drop Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.1.1 Proto:1 ICMP Type:8 ICMP Code:0.

May 19 20:37:08 2010: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from 192.168.2.1 to 172.16.31.196, with Protocol Number:1 ICMP code 3 and ICMP type 3. Reason: no flow matching payload of ICMP Error.

To generate an ICMP protocol log, an ACL rule has to be applied and logging has to be enabled.

For example, the following commands has to be executed.

```
rfs7000-37FABE(config-ip-acl-test)#permit icmp any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

25.1.14 SSH connection log

A SSH connection is enabled on the controller using factory settings.

Running primary software, version 5.0.0.0-81243X

Alternate software Secondary, version 5.0.0.0-070D

Software fallback feature is enabled

System bootup time (via /proc/uptime) was 126.10 92.38

Please press Enter to activate this console. May 19 20:47:33 2010: %DOT11-5-COUNTRY_CODE: Country of operation configured to in [India]

May 19 20:47:34 2010: %DIAG-6-NEW_LED_STATE: LED state message AP_LEDS_ON from module DOT11

May 19 20:47:34 2010: KERN: vlan1: add 01:00:5e:00:00:01 mcast address to master interface.

May 19 20:47:34 2010: %NSM-4-IFUP: Interface vlan2 is up

May 19 20:47:34 2010: KERN: vlan2: add 01:00:5e:00:00:01 mcast address to master interface.

May 19 20:47:34 2010: %NSM-4-IFUP: Interface vlan172 is up

May 19 20:47:34 2010: KERN: vlan172: add 01:00:5e:00:00:01 mcast address to master interface.

May 19 20:47:34 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1

May 19 20:47:34 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/sshd"

May 19 20:47:34 2010: %DAEMON-3-ERR: dhcrelay: idataplane enabled

nterface allocatCCB:21:Firewall enabled

e : vlan1

May 19 20:47:34 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan2

May 19 20:47:34 2010: %KERN-4-WARNING: dataplane enabled.

May 19 20:47:34 2010: %DATAPLANE-5-FWSTARTUP: Firewall enabled.

May 19 20:47:39 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Drop Packet Src MAC:<00-19-B9-6B-DA-77> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst IP:192.168.1.1 Proto:6 Src Port:3327 DstPort:22.

25.1.15 Allowed/Dropped Packets Log

The following example displays disposition information regarding allow/deny packets.

Allow Packets

CCB:0:Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:137 Dst Port:137

CCB:0:Matched ACL:ftpuser:ip Rule:1 Disposition:**Allow** Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:1029 Dst Port:53

CCB:May 19 18:14:3220100: %DATAPLAN:-5-LOGRULEHIT: Matched ACL:ftpuer:aip Rule:1 Ditcposition:Allow hedacket Src MAC: 00-11-25-14-D9-A2> Dst MAC:<00-5-70-81-9C1-6A> thertLype:0x0800:Src IP:192.168..102 Dsft IP:192t168.2.1 Proto:1p Src Port:137 Dut Port:137.

ser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:1029 Dst Port:53

Drop/Deny Packets

CCB:0:Matched ACL:ftpuser:ip Rule:0 Disposition:**Drop** Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:137 Dst Port:137

May 19 20:41:28 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0 Disposition:Drop Packet Src MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:137 Dst

To generate anallow/deny protocol log, acl rule has to be applied and logging has to be enabled.

For example, the following commands has to be executed:

```
rfs7000-37FABE(config-ip-acl-test)#permit ip any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
rfs7000-37FABE(config-ip-acl-test)#deny ip any any log rule-precedence 20
rfs7000-37FABE(config-ip-acl-test)#
```

APPENDIX 26 Controller Managed WLAN Use Case

This section describes the activities required to configure a controller managed WLAN. Instructions are provided using the controller CLI to allow an administrator to define the WLAN using the desired interface.

- Creating a First Controller managed WLAN
  - Assumptions
  - Design
  - Using the Command Line Interface to Configure the WLAN

26.1 Creating a First Controller Managed WLAN

It is assumed you have a RFS4000 wireless controller with the latest build available from Motorola. It is also assumed you have one an AP7131 model Access Point and one AP650 model Access Point, both with the latest firmware avilable from Mototrola.

Upon completion, you will have created a WLAN on a RFS4000 model wireless controller using a DHCP server to allocate IP addresses to associated wireless clients.

26.1.1 Assumptions

Creating a First Controller Managed WLAN

Verify the following conditions have been satisfied before attempting the WLAN configuration activities described in this section.

1. It is assumed the wireless controller has the latest firmware version available from Motorola.
2. It is assumed the AP7131 and AP650 Access Points also have the latest firmware version available from Motorola.
3. It is assumed there are no previous configurations on the wireless controller or Access Point and default factory configurations are running on the devices.
4. It is assumed you have administrative access to the wireless controller and Access Point CLI.
5. It is assumed the individual administrating the network is a professional network installer.

26.1.2 Design

Creating a First Controller Managed WLAN

This section defines the network design being implemented.

Figure 26-1 *Network Design*

This is a simple deployment scenario, with the Access Points connected directly to the wireless controller. One wireless controller port is connected to an external network.

On the RFS4000 wireless controller, the GE1 interface is connected to an external network. Interfaces GE3 and GE4 are used by the access points.

On the external network, the controller is assigned an IP address of 192.168.10.188. The wireless controller acts as a DHCP server for the wireless clients connecting to it, and assigns IP addresses in the range of 172.16.11.11 to 172.16.11.200. The rest of IPs in the range are reserved for devices requiring static IP addresses.

26.1.3 Using the Command Line Interface to Configure the WLAN

Creating a First Controller Managed WLAN

These instructions are for configuring your first WLAN using the Wireless Controller's *command line interface* (CLI).

Use a serial console cable when connecting to the wireless controller for the first time. Set the following configuration when using the serial connection.

- Bits per second: *19200*
- Data Bit**:** *8*
- Parity**:** *None*
- Stop Bit: *1*
- Flow Control: *None*

The general steps involved in creating a WLAN on a wireless controller can be summarized as:

1. *Logging Into the Controller for the First Time*
2. *Creating a RF Domain*
3. *Creating a Wireless Controller Profile*
4. *Creating an AP Profile*
5. *Creating a DHCP Server Policy*

26.1.3.1 Logging Into the Controller for the First Time

Using the Command Line Interface to Configure the WLAN

When powering on the wireless controller for the first time, you are prompted to replace the existing administrative password. The credentials for logging into the wireless controller for the first time are:

- User Name: *admin*
- Password: *motorola*

Ensure the new password created is strong enough to provide adequate security for the controller managed network.

26.1.3.2 Creating a RF Domain

Using the Command Line Interface to Configure the WLAN

A RF Domain is a collection of configuration settings specific to devices located at the same physical deployment, such as a building or a floor. Create a RF Domain and assign the country code where the devices are deployed. This is a mandatory step, and the devices will not function as intended if this step is omitted.

The instructions in this section must be performed from the Global Configuration mode of the wireless controller. To navigate to this mode,

```
RFS4000>enable
RFS4000#
RFS4000#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RFS4000(config)#
```

Create the RF Domain using the following commands:

```
RFS4000(config)#rf-domain RFDOMAIN_UseCase1
RFS4000(config-rf-domain-RFDOMAIN_UseCase1)#
```

This command creates a profile with the name RFDOMAIN_UseCase1.

Set the country code for the RF Domain.

```
RFS4000(config-rf-domain-RFDOMAIN_UseCase1)#country-code us
```

This sets the country code for this RF Domain. Save this change and exit the RF Domain profile context.

```
RFS4000(config-rf-domain-RFDOMAIN_UseCase1)#commit write
RFS4000(config-rf-domain-RFDOMAIN_UseCase1)#exit
RFS4000(config)#
```

To define the wireless controller's physical location, use the same RF Domain configuration.

```
RFS4000(config)#self
RFS4000(config-device-03-14-28-57-14-28)#
RFS4000(config-device-03-14-28-57-14-28)#use rf-domain RFDOMAIN_UseCase1
```

Commit the changes and write to the running configuration. Exit this context.

```
RFS4000(config-device-03-14-28-57-14-28)#commit write
RFS4000(config-device-03-14-28-57-14-28)#exit
RFS4000(config)#
```

26.1.3.3 Creating a Wireless Controller Profile

Using the Command Line Interface to Configure the WLAN

The first step in creating a WLAN is to configure a profile defining the parameters that must be applied to a wireless controller.

To create a profile:

```
RFS4000(config)#profile rfs4000 RFS4000_UseCase1
RFS4000(config-profile-RFS4000_UseCase1)#
```

This creates a profile with the name RFS4000_*UseCase1* and moves the cursor into its context. Any configuration made under this profile is available when it's applied to a device.

Configure a VLAN

Create the VLAN to use with the WLAN configuration. This can be done using the following commands:

```
RFS4000(config-profile-RFS4000_UseCase1)#interface vlan 2
RFS4000(config-profile-RFS4000_UseCase1-if-vlan2)#ip address 172.16.11.1/24
```

The above command assigns the IP address 172.16.11.1 with the mask of 255.255.255.0 to VLAN2. Exit the VLAN2 context.

```
RFS4000(config-profile-RFS4000_UseCase1-if-vlan2)#exit
RFS4000(config-profile-RFS4000_UseCase1)#
```

The next step is to assign this newly created VLAN to a physical interface. In this case, VLAN 2 is mapped to GE3 and GE4 to support two Access Points, an AP650 and an AP7131. The AP650 is connected to the gigabit interface GE3 and the AP7131 to the GE4 interface.

```
RFS4000(config-profile-RFS4000_UseCase1)#interface ge 3
RFS4000(config-profile-RFS4000_UseCase1-if-ge3)#
```

Map VLAN 1 to this interface. This assigns the IP address to the selected physical interface.

```
RFS4000(config-profile-RFS4000_UseCase1-if-ge3)#switchport access vlan 2
RFS4000(config-profile-RFS4000_UseCase1-if-ge3)#exit
RFS4000(config-profile-RFS4000_UseCase1)#
```

Similarly, map the defined VLAN 1 to the GE4 interface.

```
RFS4000(config-profile-RFS4000_UseCase1)#interface ge 4
RFS4000(config-profile-RFS4000_UseCase1-if-ge4)#switchport access vlan 2
RFS4000(config-profile-RFS4000_UseCase1-if-ge4)#exit
RFS4000(config-profile-RFS4000_UseCase1)#
```

Exit the profile and save it.

```
RFS4000(config-profile-RFS4000_UseCase1)#exit
RFS4000(config)#commit write
```

Configure the Wireless Controller to use the Profile

Before the wireless controller can be further configured, the profile must be applied to the wireless controller.

```
RFS4000(config)#self
RFS4000(config-device-03-14-28-57-14-28)#
RFS4000(config-device-03-14-28-57-14-28)#use profile RFS4000_UseCase1
RFS4000(config-device-03-14-28-57-14-28)#exit
RFS4000(config)#commit write
```

Create a WLAN

Use the following commands to create a WLAN.

```
RFS4000(config)#wlan 1
RFS4000(config-wlan-1)#
```

Configure the SSID for the WLAN. This is the value that identifies and helps differentiate this WLAN.

```
RFS4000(config-wlan-1)#ssid WLAN_USECASE_01
```

Enable the SSID to be broadcast so wireless clients can find it and associate.

```
RFS4000(config-wlan-1)#broadcast-ssid
```

Associate the VLAN to the WLAN and exit.

```
RFS4000(config-wlan-1)#vlan 2
RFS4000(config-wlan-1)#exit
```

Commit the Changes

Once these changes have been made, they have to be committed before proceeding.

```
RFS4000(config)#commit write
```

26.1.3.4 Creating an AP Profile

Using the Command Line Interface to Configure the WLAN

An AP profile provides a method of applying common settings to access points of the same model. The profile significantly reduces the time required to configure access points within a large deployment. For more information, see:

- *Creating an AP650 Profile*
- *Creating an AP7131 Profile*

26.1.3.4.1 Creating an AP650 Profile

Creating an AP Profile

An AP650's firmware is updated directly by its associated wireless controller. The process is automatic, and no intervention is required. To create a profile for use with an AP650:

```
RFS4000(config)#profile ap650 AP650_UseCase1
RFS4000(config-profile-AP650_UseCase1)#
```

Assign the access point to be a member of the same VLAN defined in *Creating an AP Profile on page 26-10*. In this section, the VLAN was defined as VLAN 2. Configure the Access Point to be a member of VLAN 2.

```
RFS4000(config-profile-AP650_UseCase1)#interface vlan 2
RFS4000(config-profile-AP650_UseCase1-if-vlan2)#
```

Configure this VLAN to use DHCP, so any device that is associated using this Access Point is automatically assigned a unique IP address. Once completed, exit this context.

```
RFS4000(config-profile-AP650_UseCase1-if-vlan2)#ip address dhcp
RFS4000(config-profile-AP650_UseCase1-if-vlan2)#exit
```

The VLAN has to be mapped to a physical interface on the Access Point. Since the only available physical interface on the AP650 is GE1, this VLAN is mapped to it.

```
RFS4000(config-profile-AP650_UseCase1)#interface ge 1
RFS4000(config-profile-AP650_UseCase1-if-ge1)#switchport access vlan 2
RFS4000(config-profile-AP650_UseCase1-if-ge1)#exit
```

Before a WLAN can be implemented, it has to be mapped to a radio on the Access Point. An AP650 has 2 radios, in this scenario, both radios are utilized.

```
RFS4000(config-profile-AP650_UseCase1)#interface radio 1
RFS4000(config-profile-AP650_UseCase1-if-radio1)#wlan 1
RFS4000(config-profile-AP650_UseCase1-if-radio1)#exit
RFS4000(config-profile-AP650_UseCase1)#interface radio 2
RFS4000(config-profile-AP650_UseCase1-if-radio2)#wlan 1
RFS4000(config-profile-AP650_UseCase1-if-radio2)#exit
RFS4000(config-profile-AP650_UseCase1)#
```

Commit the changes made to this profile and exit.

```
RFS4000(config-profile-AP650_UseCase1)#commit write
RFS4000(config-profile-AP650_UseCase1)#exit
RFS4000(config)#
```

Apply this Profile to the Discovered AP650

Access the discovered Access Point using the following command. The discovered device's MAC address is used to access its context.

```
RFS4000(config)#ap650 00-A0-F8-00-00-01
RFS4000(config-device-00-A0-F8-00-00-01)#
```

Assign the AP profile to this AP650 Access Point.

```
RFS4000(config-device-00-A0-F8-00-00-01)#use profile AP650_UseCase1
RFS4000(config-device-00-A0-F8-00-00-01)#commit write
```

Apply the RF Domain profile to the AP

Apply the previously created RF Domain to enable a country code to be assigned to the discovered Access Point. A discovered Access Point only works properly if its country code is the country code of its associated wireless controller.

```
RFS4000(config-device-00-A0-F8-00-00-01)#use rf-domain RFDOMAIN_UseCase1
RFS4000(config-device-00-A0-F8-00-00-01)#commit write
RFS4000(config-device-00-A0-F8-00-00-01)#exit
RFS4000(config)#
```

26.1.3.4.2 Creating an AP7131 Profile

Creating an AP Profile

To create a profile for use with an AP7131:

```
RFS4000(config)#profile ap7131 AP7131_UseCase1
RFS4000(config-profile-AP7131_UseCase1)#
```

Set the Access Point to be a member of the same VLAN defined in *Creating an AP Profile on page 26-10*. In this section, the VLAN was defined as VLAN 2. Configure the Access Point to be a member of the VLAN 2.

```
RFS4000(config-profile-AP7131_UseCase1)#interface vlan 2
RFS4000(config-profile-AP7131_UseCase1-if-vlan2)#
```

Configure this VLAN to use DHCP, so any device associated using this Access Point is automatically assigned a unique IP address. Once completed, exit this context.

```
RFS4000(config-profile-AP7131_UseCase1-if-vlan2)#ip address dhcp
RFS4000(config-profile-AP7131_UseCase1-if-vlan2)#exit
```

The configured VLAN has to be mapped to a physical interface on the Access Point. Map VLAN1 to the GE1 and GE2 interfaces on the AP7131. To configure the GE1 interface:

```
RFS4000(config-profile-AP7131_UseCase1)#interface ge 1
RFS4000(config-profile-AP7131_UseCase1-if-ge1)#switchport access vlan 2
RFS4000(config-profile-AP7131_UseCase1-if-ge1)#exit
```

Similarly configure the GE2 interface.

```
RFS4000(config-profile-AP7131_UseCase1)#interface ge 2
RFS4000(config-profile-AP7131_UseCase1-if-ge2)#switchport access vlan 2
RFS4000(config-profile-AP7131_UseCase1-if-ge2)#exit
```

Before the WLAN can be implemented, it has to be mapped to the physical radio on the Access Point. An AP7131 has 3 radios (on certain models), two of which can be configured for WLAN support. In this scenario, two radios are used.

```
RFS4000(config-profile-AP7131_UseCase1)#interface radio 1
RFS4000(config-profile-AP7131_UseCase1-if-radio1)#wlan 1
RFS4000(config-profile-AP7131_UseCase1-if-radio1)#exit
RFS4000(config-profile-AP7131_UseCase1)#interface radio 2
RFS4000(config-profile-AP7131_UseCase1-if-radio2)#wlan 1
RFS4000(config-profile-AP7131_UseCase1-if-radio2)#exit
RFS4000(config-profile-AP7131_UseCase1)#
```

Commit the changes made to the profile and exit this context.

```
RFS4000(config-profile-AP7131_UseCase1)#commit write
RFS4000(config-profile-AP7131_UseCase1)#exit
RFS4000(config)#
```

Apply this Profile to the Discovered AP7131

Access the discovered Access Point using the following command. The discovered device's MAC address is used to access its context.

```
RFS4000(config)#ap7131 00-23-68-16-C6-C4
RFS4000(config-device-00-23-68-16-C6-C4)#
```

Assign the AP profile to this Access Point.

```
RFS4000(config-device-00-23-68-16-C6-C4)#use profile AP7131_UseCase1
RFS4000(config-device-00-23-68-16-C6-C4)#commit write
```

Apply the RF Domain profile to the AP

Apply the previously created RF Domain to enable a country code to be assigned to the discovered Access Point. A discovered Access Point only works properly if its country code is the same as its associated wireless controller.

```
RFS4000(config-device-00-23-68-16-C6-C4)#use rf-domain RFDOMAIN_UseCase1
RFS4000(config-device-00-23-68-16-C6-C4)#commit write
RFS4000(config-device-00-23-68-16-C6-C4)#Exit
RFS4000(config)#
```

26.1.3.5 Creating a DHCP Server Policy

Using the Command Line Interface to Configure the WLAN

The DHCP Server Policy defines the parameters required to run a DHCP server on the wireless controller and assign IP addresses automatically to devices that associate. Configuring DHCP enables the reuse of a limited set of IP addresses.

To create a DHCP server policy:

```
RFS4000(config)#dhcp-server-policy DHCP_POLICY_UseCase1
RFS4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#
```

Table 26.1 displays how IP addresses are used.

Table 26.1 *IP Address Usage*

IP Range	*Usage*
172.16.11.1 till 172.16.11.10	Reserved for devices that require a static IP address
172.16.11.11 till 172.16.11.200	Range of IP addresses that can be assigned using the DHCP server.
172.16.11.201 till 172.16.11.254	Reserved for devices that require a static IP address

In the table, the IP address range of 172.16.11.11 to 172.16.11.200 is available using the DHCP server. To configure the DHCP server:

```
RFS4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#dhcp-pool
DHCP_POOL_USECASE1_01
RFS4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#
```

Configure the address range as follows:

```
RFS4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#address range 172.16.11.11 172.16.11.200
RFS4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#
```

Configure the IP pool used with a network segment. This starts the DHCP server on the specified interface.

```
RFS4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#network 172.16.11.0/24
RFS4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#exit
RFS4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#exit
RFS4000-37FABE(config)#commit write
```

Configure the RFS4000 to use the DHCP Policy

For the DHCP to work properly, the new DHCP Server Policy must be applied to the wireless controller. To apply the DHCP Server Policy to the wireless controller:

```
RFS4000-37FABE(config)#self
RFS4000-37FABE(config-device-03-14-28-57-14-28)#use dhcp-server-policy
DHCP_POLICY_UseCase1
RFS4000-37FABE(config-device-03-14-28-57-14-28)#commit write
RFS4000-37FABE(config-device-03-14-28-57-14-28)#exit
RFS4000-37FABE(config)#
```

26.1.3.6 Completing and Testing the Configuration

Using the Command Line Interface to Configure the WLAN

A wireless client must be configured to associate with the controller managed WLAN. The following information must be defined:

- SSID: `WLAN_USECASE_01`
- Country: Same as the country configured in *Creating a RF Domain on page 26-7*. In this scenario, the country code is set to US.
- Mode: Infrastructure

With the WLAN set to beacon, use the wireless client's discovery client to discover the configured WLAN and associate.

MOTOROLA

モトローラ・ソリューションズ株式会社 http://www.motorolasolutions.com/JP
〒106-0032　東京都港区六本木一丁目8番7号 アーク八木ヒルズ
TEL. (03)6365-7000　FAX. (03)3582-5673

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.
© 2011 Motorola Solutions, Inc. All Rights Reserved.

72E-152229-01 Revision B May 2011